310201604
YM

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００３年 １月２０日

出願番号
Application Number: 特願２００３－０１０５０９

[ST.10/C]: [ＪＰ２００３－０１０５０９]

出願人
Applicant(s): 株式会社日立製作所

U.S. Appln. Filed 7-8-03
Inventor: Y. Takamoto et al
Mattingly Stanger & Malur
Docket H-1105

２００３年 ４月２５日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０３０７３３

【書類名】　特許願
【整理番号】　H02016041A
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　高本　良史
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　山▲崎▼　康雄
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【電話番号】　03-3212-1111
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークストレージ装置

【特許請求の範囲】

【請求項１】

ネットワークを介して複数のクライアントにストレージを提供するネットワークストレージ装置において、

該ネットワークストレージ装置はディスク装置を有する第一の装置と複数のクライアントを接続する第二の装置から構成され、

該第一の装置は該第二の装置に上記ディスク装置の領域を割り当て、該第二の装置は該第一の装置によって割り当てられた上記領域をクライアントに割り当てるとともに、該第二の装置は上記複数のクライアントを示す複数のネットワークアドレスからのリクエストを受信し、該複数のネットワークアドレスを単一のネットワークアドレスに変換し、該第一の装置に転送することを特徴とするネットワークストレージ装置。

【請求項２】

該第二の装置は、あらかじめ設定された該第一の装置から割り当てられた領域名を、クライアントからのアクセス要求に含まれるファイル名に追加し、該第一の装置に転送することを特徴とする請求項１記載のネットワークストレージ装置。

【請求項３】

該第二の装置起動時に該第二の装置固有の装置識別子を暗号化した後に該第一の装置に転送し、該第一の装置は、該第二の装置から転送された装置識別子を復号化すると共に該第一の装置内に格納されたアクセスを許可する装置が記載されたテーブルと該第二の装置から転送された装置識別子とを比較し、該テーブルに記載された装置識別子であれば接続を許可することを特徴とする請求項２記載のネットワークストレージ装置。

【請求項４】

該第一の装置は、定期的に該第二の装置に対して該装置識別子の転送を要求し、該第二の装置から応答が無い場合あるいは、該第一の装置内に格納されたアク

セスを許可する装置が記載されたテーブルと一致しない場合は、該第二の装置に割り当てた領域に対するアクセスを禁止することを特徴とする請求項３記載のネットワークストレージ装置。

【請求項５】

該第一の装置は、該第二の装置起動時に該第二の装置に割り当てられた領域名を該第二の装置に転送することを特徴とする請求項２記載のネットワークストレージ装置。

【請求項６】

該第一の装置は、該第二の装置起動時に該第二の装置に、該第二の装置が使用することができる容量を通知し、該第二の装置はクライアントの書き込み要求時に該使用することができる容量を超えていないかどうかを判定し、超えた場合はクライアントの書き込み要求を拒絶することを特徴とする請求項５記載のネットワークストレージ装置。

【請求項７】

該第２の装置は、クライアントの書き込みあるいは読み込み要求を暗号化し、該第一の装置に転送することを特徴とする請求項２記載のネットワークストレージ装置。

【請求項８】

該第二の装置は、複数の該第二の装置との間でクライアントのファイルを転送する際に、異なるネットワーク間のファイル転送かどうかを判断し、異なるネットワーク間のファイル転送の場合は、該ファイルの管理情報に記載されたユーザ識別子を変換することを特徴とする請求項２記載のネットワークストレージ装置。

【請求項９】

該第二の装置は、該ファイルの転送の転送とともに、ファイルの転送元の第二の装置は転送したクライアントに関する管理情報を削除し、転送先の第二の装置はクライアントに関する管理情報を追加することを特徴とする請求項８記載のネットワークストレージ装置。

【請求項１０】

該第二の装置は、該第一の装置に内蔵することを特徴とする請求項２記載のネットワークストレージ装置。

【請求項１１】

複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、

複数のディスク装置を管理するネットワークファイル装置と、

上記クライアントからの上記ディスク装置へのアクセス要求を中継し、該クライアントのアドレスを自己のアドレスに変換して上記ディスク装置へアクセスするクライアント管理装置を有する、ネットワークストレージ装置。

【請求項１２】

複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、

複数のディスク装置を管理するネットワークファイル装置と、

上記クライアントからの上記ディスク装置へのアクセス要求を中継するクライアント管理装置を有し、

上記ネットワークファイル装置は、上記ディスク装置の所定の領域を上記クライアント管理装置に割り当て、

上記クライアント管理装置は、自己に割り当てられた上記所定の領域を分割して上記複数のクライアントに割り当てる、ネットワークストレージ装置。

【請求項１３】

上記ネットワークファイル装置は、上記ディスク装置の情報の少なくとも一部のコピー情報を蓄積する１次キャッシュを有し、

上記クライアント管理装置は、上記１次キャッシュに蓄積されたコピー情報のうち、自己に割り当てられた上記所定の領域に対応する部分を蓄積する２次キャッシュを有する、請求項１２記載のネットワークストレージ装置。

【請求項１４】

上記ネットワークファイル装置とネットワークストレージ装置は、単一の装置として構成されているか、または、ネットワークを介して接続される分離した装置として構成されている、請求項１２記載のネットワークストレージ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はネットワークストレージ装置におけるクライアントの効率的な管理方法に関する。

【０００２】

【従来の技術】

【特許文献１】

特開２００２－１９６９６１

【特許文献２】

特開２００２－１３２４５５

【特許文献３】

特開２００１－６７１８７

ストレージの大容量化、低価格化が進んでいる。特に磁気ディスクの分野で高い記録密度を実現する技術により、従来では実現が困難であった１筐体で数１０テラバイトの装置が実現されつつある。

【０００３】

一方、ネットワークの高性能化も進んでいる。比較的低価格で１ギガビット／秒～１０ギガビット／秒のネットワーク転送性能の製品も出てきた。従来のネットワークでは、転送性能が１０メガビット／秒～１００メガビット／秒であり、大規模なデータを転送したり、多数のユーザが使用すると転送性能がネックとなり効率の良いシステムを構築することが困難であった。しかし、１ギガビット／秒～１０ギガビット／秒のネットワークでは大規模データ転送や多数ユーザが使用しても十分実用に耐えうるシステムを構築できる。

【０００４】

こういった背景から、ストレージとネットワークを接続し、ユーザ（クライアント）からネットワークを介して共有されたストレージ上のデータにアクセスするネットワークストレージ装置の形態が注目されている。例えば、特開２００２－１９６９６１がネットワークストレージ装置の構成である。ネットワーク接続

を行う部位とサーバ処理を行う部位とデータを保存するディスク装置が単一の筐体に構成されている。クライアントは、ネットワークを介してサーバが提供する通信方法に基づいてアクセスすることで、ネットワーク上のサーバ内に格納されたデータがあたかも、自クライアント内に格納されているかのように入出力が可能となる。

【０００５】

ネットワークストレージ装置の大きな課題は大規模化に向けたストレージの管理にある。ストレージが大規模化するに従って、性能の管理やクライアントの管理が複雑化する。大規模なストレージ環境に置いて、性能の管理を簡潔化する方法については、例えば特開２００２－１３２４５５に示されているように、ネットワーク上にクライアントのデータをメモリ上にキャッシングする装置を置くことで高性能化を図る方法がある。大規模化したストレージの高性能化には、基本的に本方式のように大規模なメモリによるキャッシングにより解決するケースが多い。一方、クライアントの管理については、現状では特開２００１－６７１８７に示されるように、単一の筐体は少数の管理者がクライアントの管理を行っている。

【０００６】

【発明が解決しようとする課題】

小規模なストレージであれば、クライアント数も少なく少数の管理者でも管理可能である。しかし、磁気ディスクの大規模化に伴って１筐体の装置に数１０テラバイトものストレージが搭載できるようになっており、こうしたケースではクライアント数は数千～数万になると予想される。ここで管理とは、クライアント毎のストレージ領域の割り当てや、割り当てられた領域に対するアクセス権限の設定などである。例えば、クライアント毎に、クライアントのネットワーク（ＩＰ）アドレス、ディスク領域名（／ｕｓｅｒ／ａ）、アクセス権限（リード許可や書き込み許可）といった設定をクライアント毎に行う必要がある。また、クライアントの移動が発生した場合には、前記設定を移動したクライアントに対して再度設定し直す必要がある。

【０００７】

【課題を解決するための手段】

上記課題を解決するために、本発明は、複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、複数のディスク装置を管理するネットワークファイル装置と、クライアントからのディスク装置へのアクセス要求を中継し、クライアントのアドレスを自己のアドレスに変換してディスク装置へアクセスするクライアント管理装置を有する。これにより、ディスク装置からは複数クライアントが１つのグループに見えるので、設定をクライアント毎に行う必要がない。

【０００８】

また、本発明の他の観点は、複数のクライアントが接続されるネットワークに接続されるネットワークストレージ装置であって、複数のディスク装置を管理するネットワークファイル装置と、クライアントからのディスク装置へのアクセス要求を中継するクライアント管理装置を有し、ネットワークファイル装置は、ディスク装置の所定の領域をクライアント管理装置に割り当て、クライアント管理装置は、自己に割り当てられた所定の領域を分割して複数のクライアントに割り当てる。これにより、ディスク装置は複数クライアントからなるグループを最小単位として取り扱い、グループに対して１つの領域を割り当てるので、設定をクライアント毎に行う必要がない。

【０００９】

また、ネットワークファイル装置は、ディスク装置の情報の少なくとも一部のコピー情報を蓄積する１次キャッシュを有し、クライアント管理装置は、１次キャッシュに蓄積されたコピー情報のうち、自己に割り当てられた上記所定の領域に対応する部分を蓄積する２次キャッシュを有することとし、見かけのアクセス速度を速めることができる。ネットワークファイル装置とネットワークストレージ装置は、単一の装置として構成されていてもよいし、または、ネットワークを介して接続される分離した装置として構成してもよい。

【００１０】

さらに、上記問題を解決するために、ネットワークストレージ装置はディスク装置を有する第一の装置と複数のクライアントを接続する第二の装置から構成さ

れ、第一の装置と第二の装置とでクライアントを階層管理することで多数のクライアントを効率良く管理する。第一の装置は、第二の装置への領域の割り当てやアクセス権限の設定を行い、第二の装置はクライアント毎の設定を行う。第二の装置は、通常各ネットワークエリア毎に設置され、各ネットワークエリア毎の管理だけを行う。第二の装置は、クライアントからのアクセス要求を、第一の装置に転送するが、その際第二の装置は複数のクライアントのＩＰアドレスを単一のＩＰアドレスに変換すると共に、アクセスするディスク領域名に第二の装置特有に割り当てられたディスク領域名を追加する。

【００１１】

【発明の実施の形態】

［実施例１］

以下、本発明に係るクライアント管理方法の実施例１を図面に示し、さらに詳細に説明する。

【００１２】

図１は、本発明によるクライアント管理方法の概略構成図を示している。１０１はクライアント管理装置であり、大きくはクライアント管理機構（１０２），クライアント管理テーブル（１０３），ＩＰアドレス変換テーブル（１２０），装置容量テーブル（１０４），キャッシュ（１１０）から構成されている。クライアント管理装置（１０１）は例えばネットワーク毎に複数設置することができ、各ネットワーク毎のクライアントが使用するディスク領域や接続許可などの管理を行う。クライアント管理機構（１２）は仮想ネットワークファイル機構（１０５），ＩＰアドレス変換機構（１０６），管理者制御機構（１０７），ネゴシエーション機構（１０８），クライアント移行機構（１０９）から構成されている。クライアント管理装置はネットワークファイル装置（１１１）に接続されている。ネットワークファイル装置（１１１）は、クライアントのデータを保持する機能を有する。ネットワークファイル装置（１１１）はネゴシエーション機構（１１２），ネットワークファイル機構（１１３），クライアント管理テーブル（１１４），キャッシュ（１１５），ディスク（１１６）から構成されている。クライアント管理装置（１０１）はネットワークファイル装置（１１１）が提供

するディスク領域をクライアントに提供すると共に、クライアントの接続許可やクライアントの管理を行う機能を有する。

【００１３】

図２は、本実施例におけるクライアント管理装置の位置づけを示している。クライアント（２０１～２０８）は各ネットワーク（２０９，２１０）に接続されている。クライアント管理装置（２１１，２１２）はネットワーク（２０９，２１０）に接続され、基幹ネットワーク（２１３）を介してネットワークファイル装置（２１４）に接続される形態である。全てのクライアント（２０１～２０８）はクライアント管理装置（２１１，２１２）を介してネットワークファイル装置（２１４）にアクセスされる。ネットワークは、ネットワークファイル装置（２１４）専用に使用される形態である。クライアント管理装置（２１１）は、ネットワーク（２０９）に接続されたクライアント（２０１～２０４）を制御・管理する。また、クライアント管理装置（２１２）は、ネットワーク（２１０）に接続されたクライアント（２０５～２０８）を制御・管理する。本実施例のクライアント管理装置により、ネットワークファイル装置の管理者は、全てのクライアント（２０１～２０８）を管理する必要はなく、クライアント管理装置（２１１，２１２）を管理するだけで済むようになる。

一方、図３はクライアント管理装置のより一般的な使用形態である。クライアント（３０１～３０８）は各ネットワーク（３０９，３１０）に接続されると共に、クライアント管理装置（３１１，３１２）もクライアント（３０１～３０８）と同様に各ネットワーク（３０９，３１０）に接続される。この形態はネットワークはネットワークファイル装置（３１４）専用ではなく、他の目的にも使用することができる。図２の形態に比べ、ネットワーク（３０９，３１０，３１３）がディスクアクセス以外の様々な用途に使用されるためセキュリティは図２の形態の方が高いと言える。クライアント管理装置（３１１）は、ネットワーク（３０９）に接続されたクライアント（３０１～３０４）を制御・管理する。また、クライアント管理装置（３１２）は、ネットワーク（３１０）に接続されたクライアント（３０５～３０８）を制御・管理する。本実施例のクライアント管理装置により、ネットワークファイル装置の管理者は、全てのクライアント（３０１

～３０８）を管理する必要はなく、クライアント管理装置（３１１，３１２）を管理するだけで済むようになる。図２における形態と効果は同じである。本実施例におけるクライアント管理装置は、図２および図３の両方に対応することができる。

【００１４】

図４は、一般的なネットワークファイル装置のクライアント管理テーブルの構造を示している。図１のクライアント管理テーブル（１０３，１１４）に対応するテーブル構造である。カラム４０１はディスク（４１０）内のディスクディレクトリ（４０４～４０６）を示している。カラム４０２は、カラム４０１で示されたディレクトリを公開するクライアントのＩＰアドレスを示している。カラム４０３はディレクトリの属性を示している。ｒｅａｄ／ｗｒｉｔｅは読み込みと書き込みを許すことを意味する。またｒｅａｄは読み込みのみ許し、書き込みは許さないことを意味する。クライアント管理テーブルには接続された全てのクライアントを記述する必要がある。ディスク容量が増大している現在では、数万クライアントを管理することもあり、クライアント管理テーブルの管理者の負担は大きい。

【００１５】

図５は、本実施例におけるクライアント管理テーブルの構造を示している。本実施例では、クライアント管理テーブルが階層化されていることが特徴である。５０９はネットワークファイル装置内のクライアント管理テーブル（１１４）を示し、５０１，５０２はクライアント管理装置（１０１）内のクライアント管理テーブル（１０３）を示している。カラム５１０はネットワークファイル装置内のディレクトリを示しており、各クライアント管理装置（５０１，５０２）へ提供するディスク領域を示している。カラム５１１はクライアント管理装置（５０１，５０２）のＩＰアドレスを示している。カラム５１２はクライアント管理装置（５０１，５０２）に対する公開属性を示している。カラム５０３，５０６はネットワークファイル装置内のディレクトリを示しており、クライアントへ提供するディスク領域を示している。カラム５０４，５０７はクライアントのＩＰアドレスを示している。カラム５０５，５０８はクライアントに対する公開属性を

示している。本実施例では、ネットワークファイル装置（５０９）の管理者は、クライアント管理装置（５０１，５０２）のみ管理すれば良くなるため、管理負荷を大幅に削減できる。また、クライアントの管理者はクライアント管理装置（５０１，５０２）によって、各ネットワークの実態に即した対応が可能となる。図１におけるクライアント管理装置（１０１）の管理者は、管理者制御機構（１０７）を介してクライアント管理装置（１０２）の制御を行う。管理者は、通常ネットワークを介して管理者制御機構（１０７）にアクセスする。この際、管理者制御機構（１０７）は、要求者に対してユーザ識別子とパスワードの入力を要求し、認証されればクライアント管理装置（１０２）の制御が可能になる。他の機能としては、後述のクライアント移行機構（１０９）に対する指示や、処理の応答結果を受け取ることもできる。

【００１６】

図６は、本実施例におけるディスクのイメージを示している。クライアントのデータは、実際は図１のディスク１１６内に格納されている。本実施例では、クライアント管理装置により単一のディスク（６０１）を、複数の仮想ディスク（６０２，６０３）を設けることができる。６０２および６０３はクライアント管理装置に対して公開された、ディスク（６０１）上のディレクトリである。しかし、クライアントには、６０２あるいは６０３はあたかも実際に存在するディスクのようにみせる機能をクライアント管理装置が有している。６０２のディレクトリを有するクライアント管理装置に管理されるクライアントの領域は６０４～６０６で示されている。また、６０３のディレクトリを有するクライアント管理装置に管理されるクライアントの領域は６０７～６０９で示されている。本機能は、主にセキュリティ向上を目的としている。従来のクライアント管理では、大規模ディスク内に多数のユーザデータが一元的に格納されていた。これでは、ディレクトリ属性の設定の間違いなどにより、より多数のクライアントに情報が漏れることになる。本実施例では、前述の通り単一ディスクを複数の仮想ディスクにみせることで、仮想ディスク間の参照を制限することができる。そのため、情報が漏洩する範囲を最小限に留めることができる。

【００１７】

以下では図を用い、本実施例の詳細を説明する。

【００１８】

図７は、仮想ネットワークファイル機構のフローを示している。ステップ７０１は、クライアントからのリクエストを受け付ける。ステップ７０２ではクライアントからのリクエストがｒｅａｄ要求なのかｗｒｉｔｅ要求なのかを判定する。ｒｅａｄ要求であればステップ７０５を実行し、ｗｒｉｔｅ要求であればステップ７０３を実行する。ステップ７０３では、書き込み要求により、該ネットワークファイル装置に割り当てられたディスク容量を算出する。これはディレクトリの容量を換算する一般的な手法により達成できる。ステップ７０４では、書き込み要求により、規定のディスク容量を超えていないかどうかチェックする。このチェックは、図１の装置容量テーブル１０４に格納された規定の容量と実際に格納しているデータ容量とこれから書き込もうとしているデータの容量からチェックする。もし、規定の容量を超えるようであればステップ７０７を実行し、容量が不足していることをクライアントに通知する。書き込みが可能であればステップ７０６を実行し、書き込み処理を行う。ステップ７０５は読み込み処理を行う。書き込み処理７０６、読み込み処理７０５は、後で詳細に説明する。本実施例では、ステップ７０４の制限を設けることによって、特定のクライアントによるディスク容量の占有を防いでいる。従来のネットワークファイル装置では、ディスクのディレクトリに対する容量制限を設けるのは困難であるが、本機能によりディスク容量を公平に分配することができるようになる。

【００１９】

図８は書き込み処理のフローを示している。ステップ８０１はディスクアドレス変換を行う。このステップは本実施例の特徴の一つである。図６に示すように、クライアント管理装置は、ディスクを仮想化する機能を有している。クライアントがディレクトリ／ｕｓｅｒ／Ａ／ｆｉｌｅ１に対して書き込みを行う場合を想定すると、クライアント管理装置は、クライアント管理装置に割り当てられたディレクトリ名である／ＨＵＢ０１をクライアントからのリクエストに追加し、／ＨＵＢ０１／ｕｓｅｒ／Ａ／ｆｉｌｅ１にディスクのアドレスを変換する。この／ＨＵＢ０１／ｕｓｅｒ／Ａ／ｆｉｌｅ１が本来のディレクトリであるが、ク

ライアントはそれを意識することはないように、ステップ８０１ではディスクアドレス（ディレクトリ）の変換を行っている。ステップ８０２では、書き込みデータをキャッシュ（１１０）に書き込み終了する。キャッシュに書き込まれたデータは、図９のキャッシュ書き出し処理により定期的に書き出しが行われる。

【００２０】

図９は、クライアント管理装置のキャッシュ（１１０）に書き込まれたデータを、ネットワークファイル装置（１１１）に書き込む処理を行う。本処理は、例えば３０秒といった定期的に実行される。ステップ９０１はキャッシュ（１１０）の空き領域判定を行う。空き領域が例えばキャッシュ（１１０）全体の２０％以上であれば、書き込み処理を行わず終了する。空き領域が少なければ、ステップ９０２を実行する。ステップ９０２では、ネットワークパケットを生成する。クライアント管理装置とネットワークファイル装置の間はネットワークで接続されている。この間のデータ転送にはネットワークパケットを生成する必要がある。ステップ９０５は、データを暗号化する。これは通信のセキュリティをさらに高めるためである。ステップ９０３ではステップ９０２で生成したネットワークパケットおよびステップ９０５で暗号化されたパケットを送信する。ステップ９０４では、正常に送信できたかどうか結果を解析する。

【００２１】

図１０は読み込み処理のフローを示している。ステップ１００１はディスクアドレス変換を示している。これは、図８のステップ８０１と同じ処理である。読み込みのファイルアドレスを実際にネットワークファイル装置に格納されているアドレスに変換する。ステップ１００２はキャッシュに所定のデータが入っているかどうかを判定する。キャッシュに所定のデータが入っていた場合はステップ１０１０を実行する。キャッシュに所定のデータが入っていなかった場合はステップ１００３を実行する。ステップ１００３は、ネットワークパケットを生成する。これは図９のステップ９０２と同じである。ステップ１００４はＩＰアドレス変換を行う。本処理は、多数のクライアントのＩＰアドレスを単一のＩＰアドレスに変換してネットワークファイル装置（１１１）に転送する機能である。本処理により、ネットワークファイル装置（１１１）は単一クライアントからの要

求のように処理できるようになる。本処理については後で詳細に説明する。ステップ１００５ではネットワークパケットをネットワークファイル装置（１１１）に転送する。ステップ１００６ではネットワークファイル装置（１１１）からデータを受け取り、状態を解析する。もし、エラーが発生していた場合はステップ１００３からリトライする。ステップ１００８では暗号化されているデータを復号化する。ステップ１００９では、読み込んだデータをキャッシュに格納し、次にアクセスされた場合はキャッシュから取り出すことで読み込み処理を高速化する。ステップ１０１０では読み込んだデータをクライアントに転送する。

【００２２】

次にＩＰアドレス変換機構について説明する。

【００２３】

図１１は、ネットワークを流れるパケットの一般的な構造を示している。１１０１から１１０４はＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットを示している。また、１１０５から１１０８は、ＩＰパケット内のデータの構造を示している。１１０１は、送信先のＩＰアドレスであり、１１０２は送信元のＩＰアドレスである。ＩＰアドレスはネットワークに接続されたクライアントやサーバなどに付けられたネットワークの識別アドレスである。ＩＰアドレスは、少なくとも同一ネットワーク内ではユニークでなければならない。クライアントとサーバ間、クライアント間、サーバ間などのネットワークによる通信時にはお互いのＩＰアドレスを指定して通信を行う。１１０３はＩＰ通信時のオプションを記述する。１１０４はＩＰのデータが格納されている。通常、ＩＰのデータ領域に直接クライアントのデータを格納することはない。ＩＰパケットは、通信中にパケットが損失してしまっても基本的には何もしない。こういった場合、ＩＰパケットが損失したかどうか、損失した場合の再送といった処理はＩＰパケットを送受信するプログラムが独自に記述する必要がある。しかし、それではネットワークにさまざまな転送方式が混在し通信の互換性が無くなったり、通信プログラムが複雑になってしまう。そこで、ＩＰよりも高機能な処理行うレイヤーを追加し、ＩＰパケットをラッピングすることでネットワークの互換性や使い勝手を向上する方法が採用されている。１１０５から１１０８のデータがそのレイヤに関す

るデータであり、通常ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）データと呼ばれている。ＩＰパケットに、再送などの機能を持ったＴＣＰデータをラッピングすることで、使い勝手や信頼性を向上することができる。１１０５は、送信先のポート番号であり、１１０６は送信元のポート番号である。ポート番号は、ファイルサービスやメールサービスなどのサービスあるいは機能に対して割り当てられる番号と、オペレーティングシステムが独自に決める番号と２種類ある。例えば、クライアントがファイルサービスをあるサーバに対して要求する場合、送信先ポートにはファイルサービスに対応する一意の番号が割り当てられ、送信元ポートはオペレーティングシステムが使用されていないユニークな番号が割り当てられる。このポート番号は、サービスレベルで相手を特定し、お互いがＴＣＰデータを間違いなく送受信するために使用される。１１０７はＴＣＰに対応したオプションが設定される。１１０８はアプリケーションデータが格納される。ファイルサービスの場合は、アプリケーションデータ（１１０８）の領域にファイル入出力データが格納されている。

【００２４】

図１２は、ＩＰアドレス変換機構のパケット送信時のフローを示している。ステップ２３０１は、送信パケット中から送信元のＩＰアドレスとポート番号を取得する。ステップ２３０２は、送信元のＩＰアドレスとポート番号をＩＰアドレス変換テーブルに格納する。

【００２５】

図１５にＩＰアドレス変換テーブルの構造を示す。カラム１３０１はクライアントのＩＰアドレスであり、カラム１３０２はクライアントのポート番号、カラム１３０３は変換後のＩＰアドレスであり、カラム１３０４は変換後のポート番号である。このテーブルは、変換後のパケットと要求元を判別するための対応表である。ステップ２３０３は、パケット中の送信元のＩＰアドレスをクライアント管理装置のＩＰアドレスに変換する。ステップ２３０４は、パケット中の送信元のポート番号を空きポート番号に変換する。本処理は使用中のポート番号をメモリ内に格納しておくことで実現可能である。ステップ２３０５は、変換後のＩＰアドレスとポート番号をＩＰアドレス変換テーブルに格納する。これらの処理

により、複数のＩＰアドレスを有するクライアントからの要求を単一のＩＰアドレスに変換することができる。

【００２６】

図１３は、ＩＰアドレス機構の受信時のフローを示している。ステップ２４０１は、送信先のＩＰアドレスとポート番号を取得する。ステップ２４０２は、ＩＰアドレス変換テーブル中からステップ２４０２で取得したＩＰアドレスとポート番号に一致するデータを検索する。ステップ２４０３は、ステップ２４０２で検索したデータのクライアントＩＰアドレス（１３０１）とクライアントポート番号（１３０２）と、受信したパケットの送信先ＩＰアドレスとポート番号とを変換する。ステップ２４０４は、ＩＰアドレス変換テーブルの項目を削除する。これらの処理は、クライアントから発行されたパケットのＩＰアドレスと送信元のポート番号の組み合わせで管理することでＩＰアドレスを変換しても要求元を一意に特定できる特性を利用したＩＰアドレス変換方法である。本処理により、ネットワークファイル装置（１１１）は、複数のクライアントが接続された環境でも、クライアント管理装置（１０１）がＩＰアドレスを１つに変換するため、領域管理が簡単になる。

【００２７】

図１４は、上記処理の動作を示している。クライアント（１２０１）はクライアント管理装置（１２２０）に接続され、クライアント管理装置（１２２０）はネットワークファイル装置（１２１２）に接続されている。クライアント（１２０１）はクライアント管理装置（１２２０）に対して読み込み要求（１２０２）を発行する。読み込み要求（１２０２）には、クライアントのＩＰアドレス１９２．１６８．０．１０とクライアントのポート番号２０００，クライアント管理のＩＰアドレス１９２．１６８．０．１００とサービスを示すポート番号８０と、クライアント（１２０１）が読み込みを要求するファイル名／ｕｓｅｒ／Ａが格納されている。クライアント（１２０１）からは、あたかもクライアント管理装置（１２２０）がディスクを有しているように見える。この要求を受けたクライアント管理装置（１２２０）は仮想ネットワークファイル機構（１２０４）により、ディスクアドレスが変換されパケット１２０６のように読み込みアドレス

に／ＨＵＢ０１が追加され／ＨＵＢ０１／ｕｓｅｒ／Ａに変換される。もし、／ＨＵＢ０１／ｕｓｅｒ／Ａがキャッシュ１２２０に格納されていた場合は、クライアント１２０１にデータが返送されるが、キャッシュ１２２０に格納されていなかった場合はＩＰアドレス変換機構（１２０８）にパケットが渡される。ここで、ＩＰアドレス変換が行われ、パケット１２１０のように、送信元アドレスはクライアント管理装置（１２２０）自身のＩＰアドレスである１９２．１６８．１０．１０に変換され、送信元ポート番号はクライアント管理装置（１２２０）内で未使用の１００００が割り当てられる。また送信先ＩＰアドレスはネットワークファイル機構（１２１２）のＩＰアドレスが設定される。この変換結果は、ＩＰアドレス変換テーブル（１２０９）に格納される。送信先ポート番号は、クライアント（１２０１）が発行した、送信先ポート番号８０と同じである。このパケット（１２１０）を受け取ったネットワークファイル装置（１２１２）は、／ＨＵＢ０１／ｕｓｅｒ／Ａのファイルを読み込み、パケット１２１１に読み込んだデータ（ｄａｔａ）を格納して直接の要求元であるクライアント管理装置（１２２０）に返送する。クライアント管理装置（１２２０）は、ネットワークファイル装置（１２１２）からパケットを受け取るとＩＰアドレス変換機構（１２０８）とＩＰアドレス変換テーブル（１２０９）により、クライアントのＩＰアドレスとクライアントが発行した時のポート番号に変換されパケット１２０７が生成される。このパケット（１２０７）は仮想ネットワークファイル機構（１２０４）を介してクライアント（１２０１）に返送される。このように、クライアント管理装置（１２２０）によって、クライアントにはあたかもディスクがクライアント管理装置（１２２０）にあるかのように見せ、ネットワークファイル装置（１２１２）には複数のクライアントが接続されたようには見せなくすることができる。

【００２８】

図１６はクライアント管理装置（１０２）におけるネゴシエーション機構（１０８）のフローを示している。ネゴシエーション機構の目的は、クライアント管理装置（１０２）とネットワークファイル装置（１１１）間の通信を正しく確立することにある。ネットワーク上を流れるパケットが第３者に見られてしまった

り、クライアントを偽ってデータを読み出そうとする行為を検出し接続できなくする処理を行う。本フローは、ネットワークファイル装置（１１１）に接続を開始するときと、ネットワークファイル装置（１１１）から一定期間毎に呼び出される。ステップ１４０１は装置識別要求かどうかを判断する。装置識別要求とは、ネットワークファイル装置（１１１）から定期的に呼び出され、ネットワークファイル装置（１１１）に対して装置識別子を転送する要求である。装置識別要求であればステップ１４０７を実行し、そうでなければステップ１４０２を実行する。ステップ１４０２以降の処理は、ネットワークファイル装置（１１１）と最初に接続する時に実行される。ステップ１４０２はネットワークファイル装置（１１１）に対してコネクションの開始を要求する。ステップ１４０３は、装置識別子を暗号化する。装置識別子とは、クライアント管理装置特有の識別子で、クライアント管理装置とネットワークファイル装置の間だけで使用される。ステップ１４０４は、ステップ１４０３で暗号化された装置識別子をネットワークファイル装置に転送する。ステップ１４０５は、ネットワークファイル装置とコネクションが確立したかどうかを判定する。これは、送信した装置識別子がネットワークファイル装置に認定された場合、コネクション許可を通知するようにすることで実現できる。コネクションが確立された場合ステップ１４０６を実行し、クライアント管理装置が使用可能な装置容量とクライアント管理装置のルートディレクトリを送信する。ルートディレクトリは、図１０のステップ１００１等で使用される。また、ネットワークファイル装置（１１１）から定期的に呼び出されるフローもある。ステップ１４０７以降は、ネットワークファイル装置（１１１）から定期的に呼び出されるフローである。このフローの目的は、ＩＰアドレスを偽ったアクセスを排除することである。ステップ１４０１以降の処理は、クライアント管理装置の起動時に実行されるが、起動後も定期的に装置識別子を送信することで常に正しい接続を保つためである。ステップ１４０７は装置識別子を暗号化する。ステップ１４０８はステップ１４０７で暗号化された装置識別子をネットワークファイル装置（１１１）に送信する。

【００２９】

図１７は、ネットワークファイル装置（１１１）におけるネゴシエーション機

構（１１２）のフローを示している。ステップ１５０１はクライアント管理装置からのコネクション要求を受け付ける。ステップ１５０２はクライアント管理装置から転送された装置識別子が格納されたデータを復号化する。ステップ１５０３は復号化された装置識別子が正しいかどうか確認し、ステップ１５０４で正しいクライアント管理装置からの要求であればステップ１５０５を実行し、正しくなかった場合はステップ１５１１で不正アクセスと判断し装置を閉塞する。ここで、閉塞の範囲は任意である。例えば、装置全体を閉塞し全てのアクセスを停止させることも考えられるし、該当するクライアント管理装置に割り当てた領域だけ停止することも考えられる。ステップ１５０５は、クライアント管理装置に対して、使用可能なディスクの容量とルートディレクトリを送信する。ステップ１５０９は一定期間処理を停止する。ステップ１５０６はクライアント管理装置に対して装置識別子を要求する。ステップ１５０７は装置識別子が正しいかどうかを確認する。ステップ１５０８で正しいクライアント管理装置からの要求であればステップ１５０９を実行し、そうでなければステップ１５１０で装置を閉塞する。こうすることで、クライアント管理装置起動後にＩＰアドレスを偽ったアクセスが発生しても、ネットワークファイル装置とクライアント管理装置しか知らない装置識別子を確認しあうことで不正アクセスを検知でき、データが不正に読まれたり改竄されることを防ぐことができる。

【００３０】

次に、本発明におけるもう一つの特徴であるユーザ移行機構について説明する。

【００３１】

図１８は、ネットワーク間でユーザが移行する場合のネットワークファイルの管理を示している。１６０１～１６０３は移行元のクライアント管理テーブルであり、１６０４～１６０６は移行先のクライアント管理テーブルである。１６１０はディスクであり、１６０８は移行元のクライアント管理装置に割り当てられたディスク領域であり、１６０９は移行先のクライアント管理装置に割り当てられたディスク領域である。１６１２は、移行元のクライアントが保有するデータであり、１６２３はデータの移行先を示している。異なるネットワーク間でクラ

イアントが移行する場合、まず、１６０７に示すようにクライアント管理テーブルの該当クライアントを移行する。その後、データの移行のため、１６１１に示すように移行元のディスク領域１６１２から該当クライアントが保有するデータを吸い上げた後、移行先であるディスク領域１６１３にデータをコピーする。データのコピーの際に、必要な処理としてユーザ識別子の変換がある。ユーザ識別子は、ネットワーク毎に決められたユーザ毎にユニークな番号である。ユーザ識別子はユーザが保有するファイル毎に設定されており、この情報はネットワークファイル機構がディスク内に格納している制御情報である。

【００３２】

図１９はファイルの管理テーブルの構造を示している。カラム１７０１はファイル名であり、カラム１７０２はユーザ識別子であり、カラム１７０３はファイルの属性を示している。ユーザ識別子１７０２はネットワーク毎にそのネットワークの管理者が定めたユーザ毎にユニークな番号であるネットワークファイル機構（１１３）はユーザ識別子を使用して、ファイルのアクセス権限を管理している。カラム１７０３はファイルの属性であり、例えば、rはリードを許可し、wは書き込みを許可するといったことを意味する。クライアント管理テーブルの更新は通常は管理者が行い、データの移行は通常はクライアント自身が行わなくてはならない。データ移行方法の一例として、まずクライアントが移行元のデータをクライアント自身にコピーする。次にクライアントはネットワークの移行を行う。この際、クライアントは移行先のネットワークの管理者から新しいユーザ識別子を教えてもらう。クライアントは、クライアント内のファイルについて、新しいユーザ識別子に変換する。この時点で、先にコピーしたファイルのユーザ識別子が新しいユーザ識別子に変換される。その後、コピーしたファイルを移行先のネットワークファイル装置（１１１）に転送し、全ての移行処理が完了する。このように、現状のクライアント移行処理はクライアント自身の負担が大きい。

【００３３】

図２０はクライアント管理装置（１０２）内のクライアント移行機構の移行元のフローを示している。ステップ１８０２は管理者から要求を受け付ける。管理者から要求とは、クライアント管理テーブル内の移行したいクライアントのリス

トなどである。ステップ１８０２は、移行先のクライアント管理装置に対して、ステップ１８０１で受け取った移行対象のクライアント情報とともに問い合わせを行う。ステップ１８０３は移行先のクライアント管理装置から、移行を了承するかどうかの応答を待つ。このとき、管理者はクライアントの移行が可能な場合、クライアント管理装置に対してクライアントの新しいユーザ識別子を通知する。ステップ１８０４は、移行が可能かどうかを判定し、移行が可能であればステップ１８０５を実行し、移行できない場合はステップ１８０９を実行する。ステップ１８０５は移行対象のクライアントのデータを読み込む。ステップ１８０６は移行先のクライアント管理装置に対して、ステップ１８０５で読み込んだデータを送信する。ステップ１８０７は移行先のクライアント管理装置から該当するクライアントのデータ移行が完了したかどうかの応答を待つ。ステップ１８０８は移行元のクライアント管理装置内のクライアント管理テーブルから、移行を終了したクライアントの情報を削除する。ステップ１８０９は、クライアント管理装置の管理者に対して、移行結果を通知する。

【００３４】

図２１はクライアント管理装置（１０２）内のクライアント移行機構の移行先のフローを示している。ステップ１９０１は移行元のクライアント管理装置から移行の要求を受け付ける。この要求には、移行元から移行したいクライアントの情報が含まれる。ステップ１９０２は、移行先のクライアント管理装置の管理者に対して、移行するかどうかを問い合わせる。ステップ１９０３は管理者からの応答を待つ。ステップ１９０４は移行可能かどうかを判断し、移行可能であればステップ１９２０を実行し、そうでないならステップ１９０９を実行する。ステップ１９２０は移行元のクライアント管理装置に対して、クライアントの移行が可能であることを通知する。ステップ１９０５は、移行元のクライアント管理装置からクライアントのデータを受信する。ステップ１９０６は受信したデータのユーザ識別子を、ステップ１８０２で通知された新しいユーザ識別子に変換する。ステップ１９０７はユーザ識別子が変換されたクライアントのデータの書き込みを行う。ステップ１９０８は、移行元のクライアント管理装置に対して、クライアントのデータの移行が完了したことを通知する。ステップ１９０９は、クラ

イアント管理装置内のクライアント管理テーブルに移行したクライアントの情報を追加する。ステップ１９１０は管理者へクライアントの移行が完了したことを通知する。これらの処理により、クライアント管理装置間でクライアント管理テーブルの更新やクライアントのデータ移行が可能となり、クライアントは移行のための処理を行う必要がなくなる。本実施例では、データ移行時にユーザ識別子を変更する手順を述べたが、ネットワークを移動しない場合はユーザ識別子は変わらないためユーザ識別子を変更する必要はない。ネットワークを判定し、同一ネットワーク内での移動であればユーザ識別子の移動は行わず、異なるネットワークの場合のみユーザ識別子の変更を行うこともできる。

【００３５】

本実施例１では、ネットワークファイル装置と、ネットワークファイル装置に接続されたクライアント管理装置において、多数のクライアントを管理する方法として、クライアント管理装置とネットワークファイル装置とでクライアントの管理を階層化することで管理負荷を低減する方法を述べている。本実施例の効果として、クライアント管理装置とネットワークファイル装置間を暗号化することで、多数のネットワーククライアントが接続されたネットワークを介しても安全にファイルアクセスができ、かつクライアント管理負荷も低減できる。また、クライアント管理装置内に設けたキャッシュにより、クライアントから頻繁にアクセスされるデータはキャッシュに格納されるため、アクセス性能を高める効果がある。ネットワークファイル装置は特定のクライアント管理装置からのみデータへの読み書きを許可する形態であるため、クライアント管理装置以外のクライアントから読み書きされることはない。そのため、クライアント管理装置を介さないアクセスがないことを保証できるため、クライアント管理装置内のキャッシュに不整合が生じることはない。また、大規模なディスク領域を複数の領域に分割し、分割したそれぞれの領域を各クライアント管理装置が管理可能となる。領域には使用可能な最大容量を設定することができるため、ネットワークファイル装置の管理者は大規模なディスク領域を管理し易くなる。

［実施例２］

実施例２では、実施例１におけるクライアント管理装置（１０２）がネットワ

ークファイル装置（１１１）に内蔵されたケースについて述べる。実施例２では、クライアント管理装置がネットワークファイル装置に内蔵されているため、大規模ディスクの管理負荷を抑えつつ、実装コストを低減することができる。

【００３６】

図２２はネットワークファイル装置（２１０１）の構成図を示している。ネットワークファイル装置（２１０１）は、クライアント管理機構（２１０２）、クライアント管理テーブル（２１０３，２１１０）、ＩＰアドレス変換テーブル（２１２０）、装置容量テーブル（２１０４）、ネットワークファイル機構（２１０９）、キャッシュ（２１１１）から構成される。ネットワークファイル装置（２１０１）には複数のディスク（２１１２）が接続されている。各構成図の動作は実施例１と同様である。ただし、実施例１における暗号化処理は、実施例２では実行しなくても構わない。これは、暗号化処理はネットワークを流れるデータを保護することが大きな目的であり、実施例２のようにクライアント管理機構（２１０２）がネットワークファイル装置（２１０１）に内蔵されている場合は、通信中のデータを第３者が見ることができないためである。そのため、実施例１に比べ暗号化の処理が削減できるため処理を高速化することができる。さらに、実施例では、各クライアント管理装置毎にキャッシュが設けられていたが、実施例２ではネットワークファイル装置が有するキャッシュを使用できるため、機構を簡単化することができる。実施例２でも、クライアントの管理方法は実施例１と同じである。ネットワークファイル装置（２１０１）の管理者は、ネットワークファイル装置（２１０１）に接続されたディスク（２１１２）の領域をクライアント管理機構（２１０２）に提供するだけであり、実際のクライアント管理はクライアント管理機構の管理者が行うことで、大規模クライアントの管理を階層化できる。クライアント管理機構は複数でも構わない。ネットワーク毎にクライアント管理機構（２１０２）を設けることで、多数のネットワーク上のクライアントを階層管理できるようになる。それぞれの管理者は、ネットワークを介して、ネットワークファイル機構（２１０９）やクライアント管理機構（２１０２）にアクセスすることができる。

【００３７】

図２３は、本発明の実施例２におけるネットワークの構成図を示している。全てのクライアント（２２０１）は、ネットワーク（２２０３）を介して直接ネットワークファイル装置（２２０４）に接続している。実施例１に比べ、簡単なネットワーク構成で本発明の効果を得ることができる。

【００３８】

【発明の効果】

本発明により、大規模なネットワークストレージのクライアントを階層管理することができ、これにより効率的なクライアント管理が行えるようになる。

【図面の簡単な説明】

【図１】

本発明の実施例１における全体構成図を示す。

【図２】

本発明のネットワーク構成の例を示す。

【図３】

本発明のネットワーク構成の例を示す。

【図４】

ネットワークファイル装置のクライアント管理情報を示す。

【図５】

実施例１におけるクライアント管理情報の構成を示す。

【図６】

実施例１におけるディスク管理の構成を示す。

【図７】

仮想ネットワークファイル機構のフローを示す。

【図８】

書き込み処理のフローを示す。

【図９】

キャッシュ書き出し処理のフローを示す。

【図１０】

読み込み処理のフローを示す。

【図１１】

ネットワークパケットの構成を示す。

【図１２】

ＩＰアドレス変換機構の送信時のフローを示す。

【図１３】

ＩＰアドレス変換機構の受信時のフローを示す。

【図１４】

実施例１におけるＩＰアドレスとファイル名の変換手順を示す。

【図１５】

ＩＰアドレス変換テーブルの構成を示す。

【図１６】

クライアント管理装置のネゴシエーション機構のフローを示す。

【図１７】

ネットワークファイル装置のネゴシエーション機構のフローを示す。

【図１８】

クライアント移行時の手順を示す。

【図１９】

ファイルの管理テーブルの構造を示す。

【図２０】

クライアント移行機構の移行元のフローを示す。

【図２１】

クライアント移行機構の移行先のフローを示す。

【図２２】

実施例２の全体構成図を示す。

【図２３】

実施例２のネットワーク構成を示す。

【符号の説明】

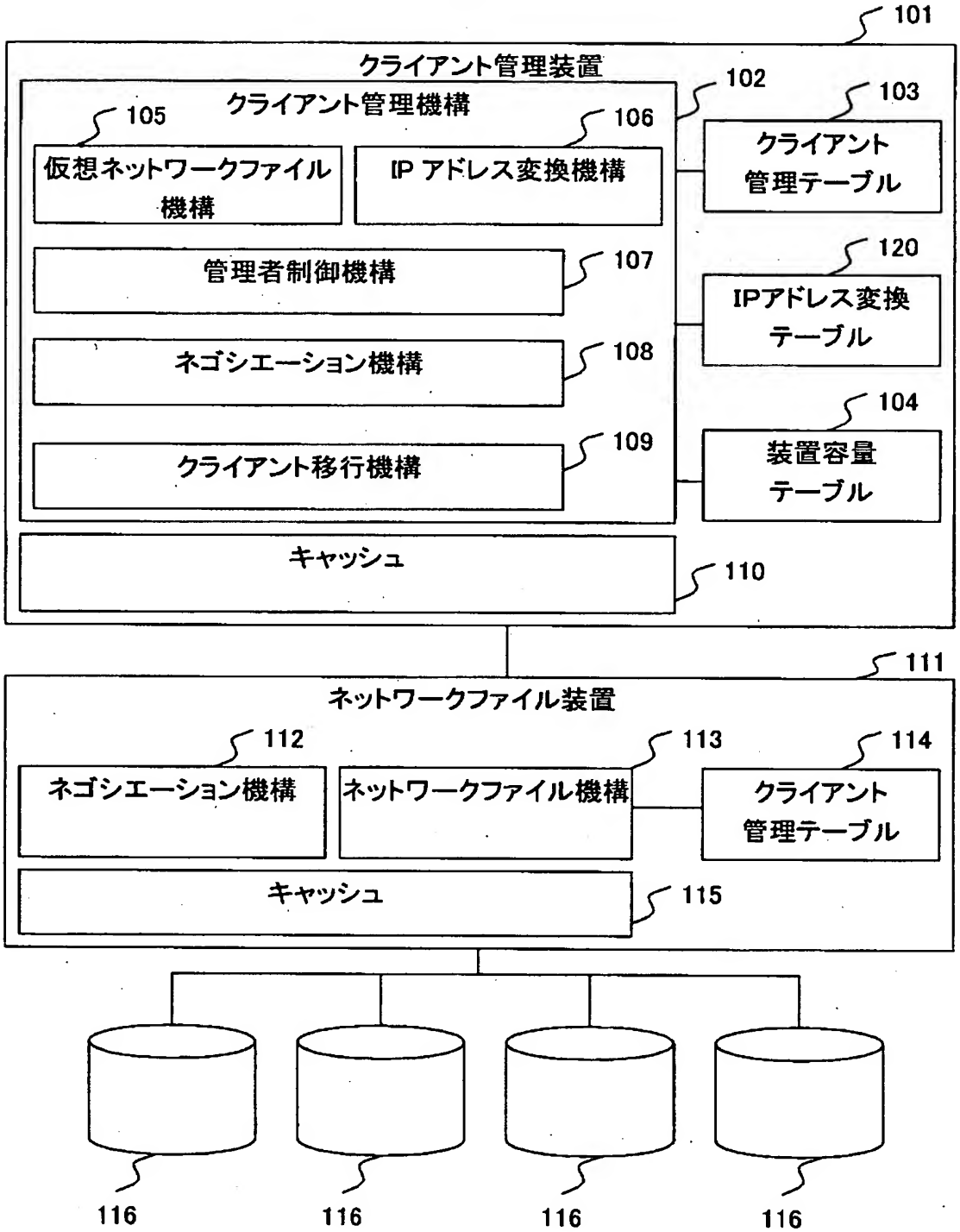
１０１はクライアント管理装置、１１１はネットワークファイル装置，１０２はクライアント管理機構，１０３および１１４はクライアント管理テーブル，１

２０はＩＰアドレス変換テーブル，１０４は装置容量テーブル，１０５は仮想ネットワークファイル機構，１０６はＩＰアドレス変換機構，１０７は管理者制御機構，１０９はクライアント移行機構，１１０および１１５はキャッシュ，１０８および１１２はネゴシエーション機構，１１３はネットワークファイル機構を示している。

【書類名】　　図面

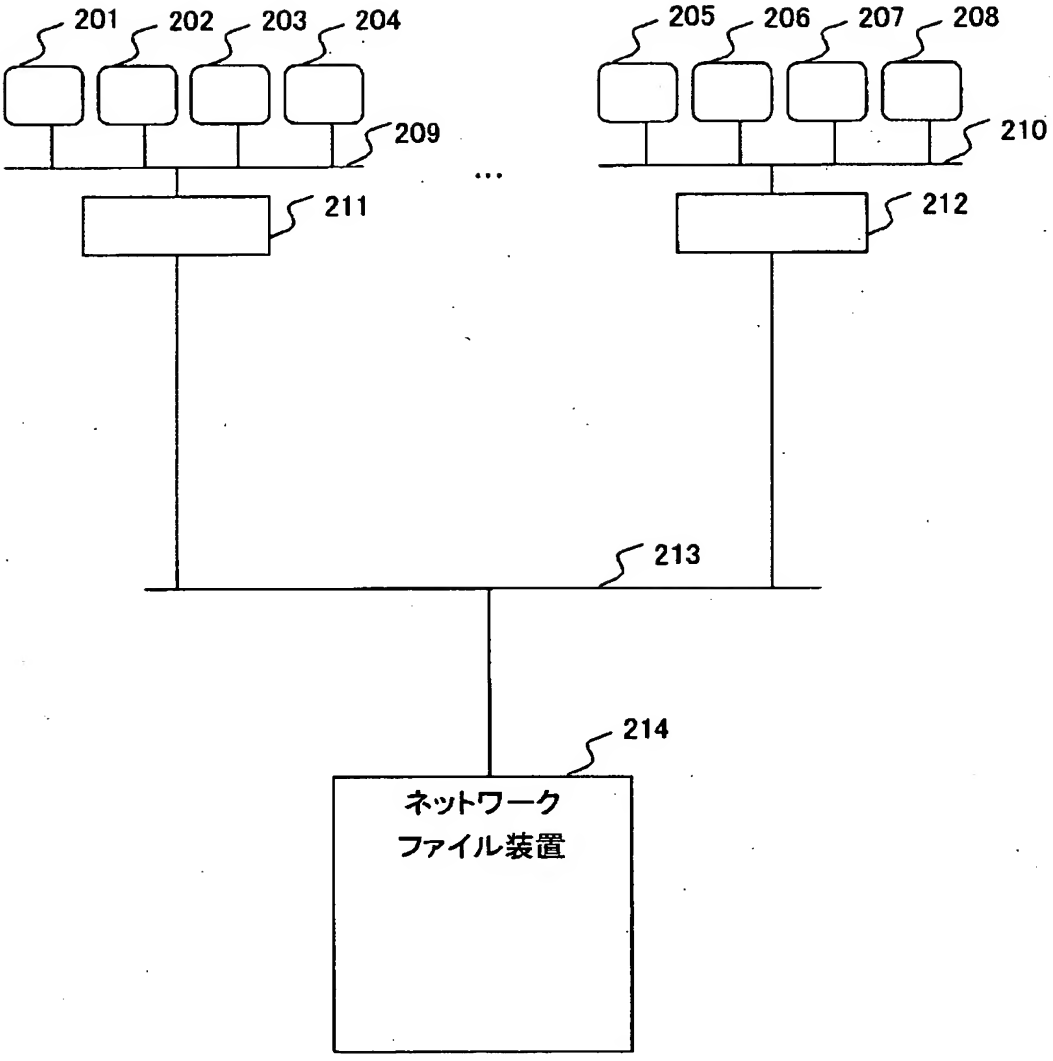
【図１】

図１


101
クライアント管理装置
クライアント管理機構
105
106
102
103
仮想ネットワークファイル機構
IP アドレス変換機構
クライアント管理テーブル
管理者制御機構
107
120
IPアドレス変換テーブル
ネゴシエーション機構
108
104
クライアント移行機構
109
装置容量テーブル
キャッシュ
110
111
ネットワークファイル装置
112
113
114
ネゴシエーション機構
ネットワークファイル機構
クライアント管理テーブル
キャッシュ
115
116
116
116
116

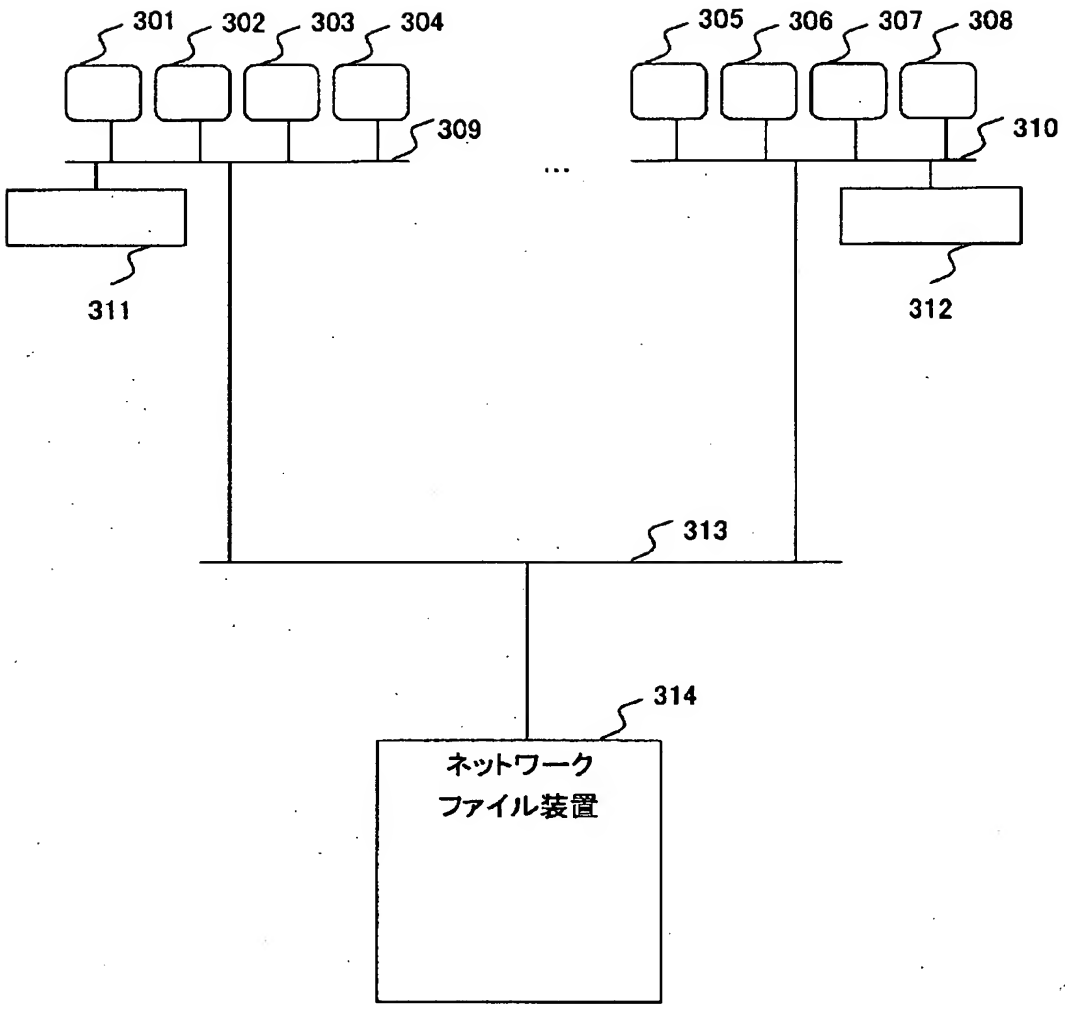
【図２】

図２


201
202
203
204
205
206
207
208
209
210
211
212
213
214
ネットワーク
ファイル装置

【図３】

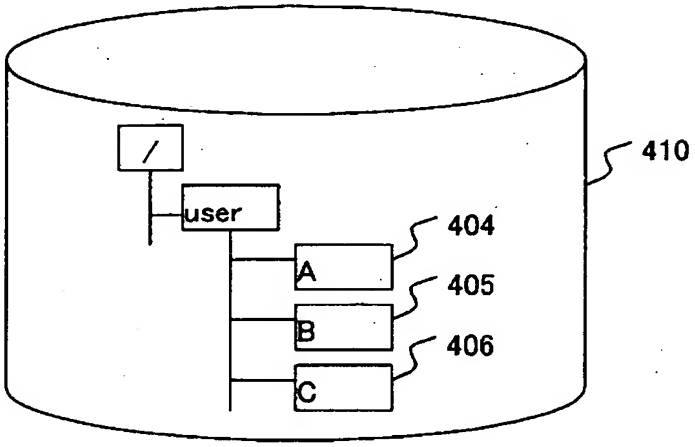
図３


301
302
303
304
305
306
307
308
309
310
311
312
313
314
ネットワーク
ファイル装置

【図４】

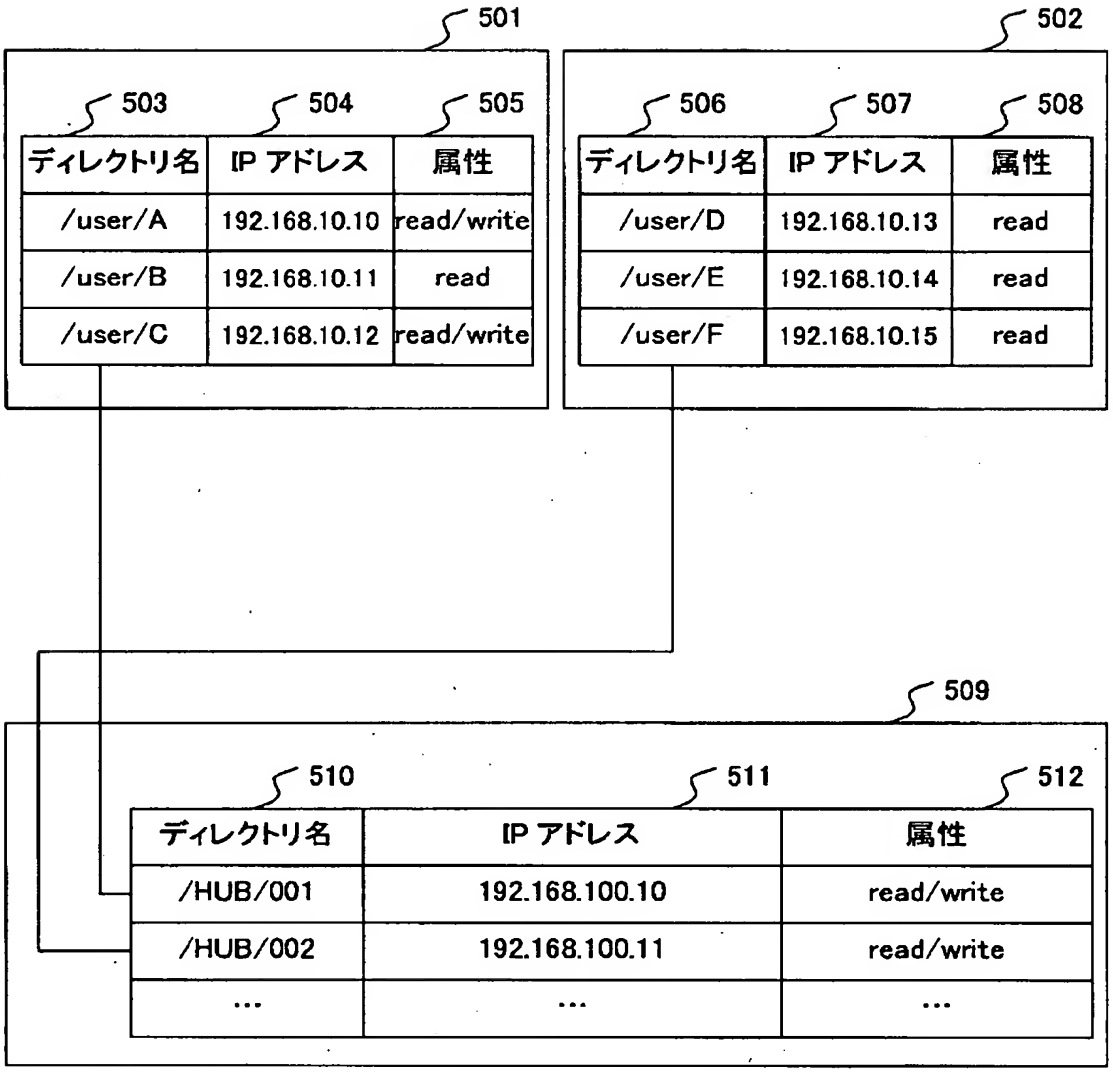
図 4

401 ディレクトリ名	402 IP アドレス	403 属性
/user/A	192.168.100.10	read/write
/user/B	192.168.100.11	read
/user/C	192.168.100.12	read/write
...	...	...



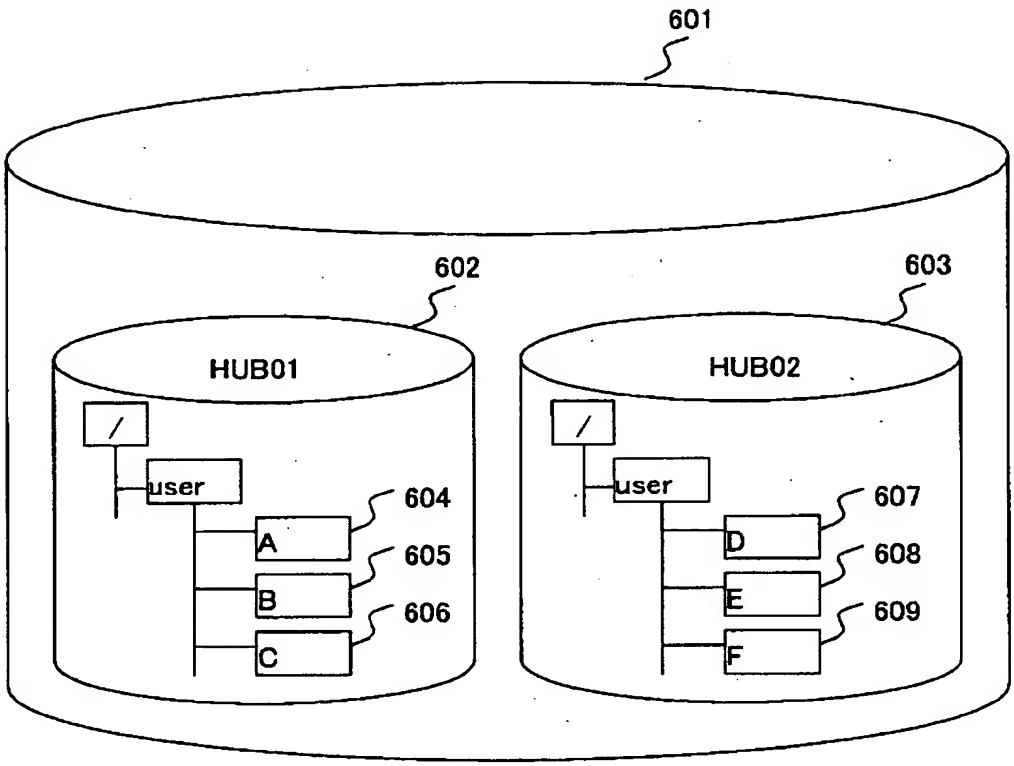
【図５】

図５


501
502
503
504
505
ディレクトリ名
IP アドレス
属性
/user/A
192.168.10.10
read/write
/user/B
192.168.10.11
read
/user/C
192.168.10.12
read/write
506
507
508
ディレクトリ名
IP アドレス
属性
/user/D
192.168.10.13
read
/user/E
192.168.10.14
read
/user/F
192.168.10.15
read
509
510
511
512
ディレクトリ名
IP アドレス
属性
/HUB/001
192.168.100.10
read/write
/HUB/002
192.168.100.11
read/write
…
…
…

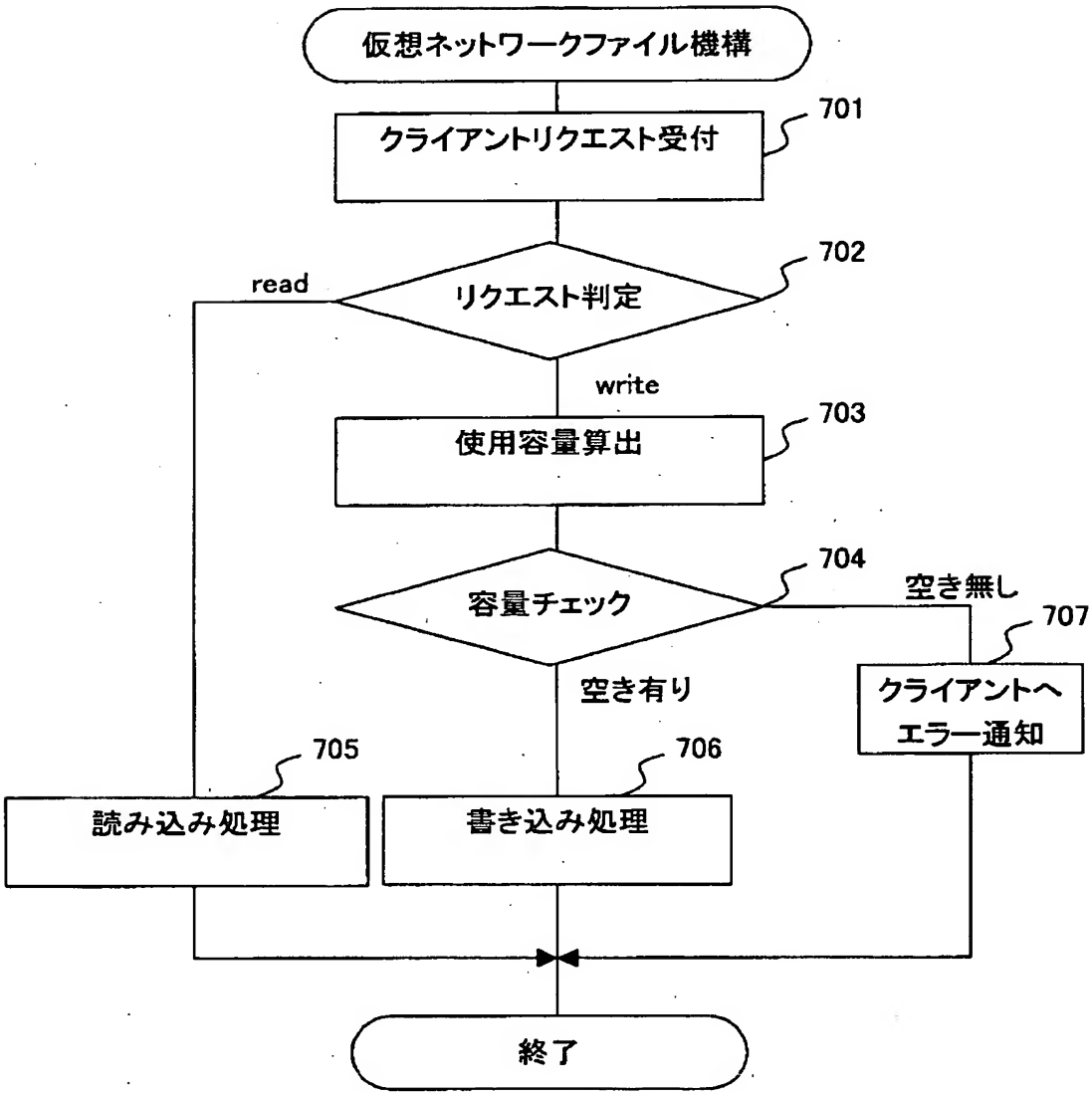
【図６】

図６


601
602
603
HUB01
HUB02
/
user
604
605
606
A
B
C
/
user
607
608
609
D
E
F

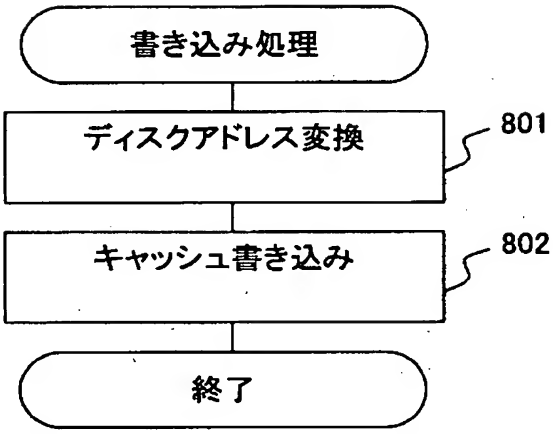
【図７】

図７


仮想ネットワークファイル機構
クライアントリクエスト受付
701
リクエスト判定
702
read
write
使用容量算出
703
容量チェック
704
空き無し
707
クライアントへ
エラー通知
空き有り
705
読み込み処理
706
書き込み処理
終了

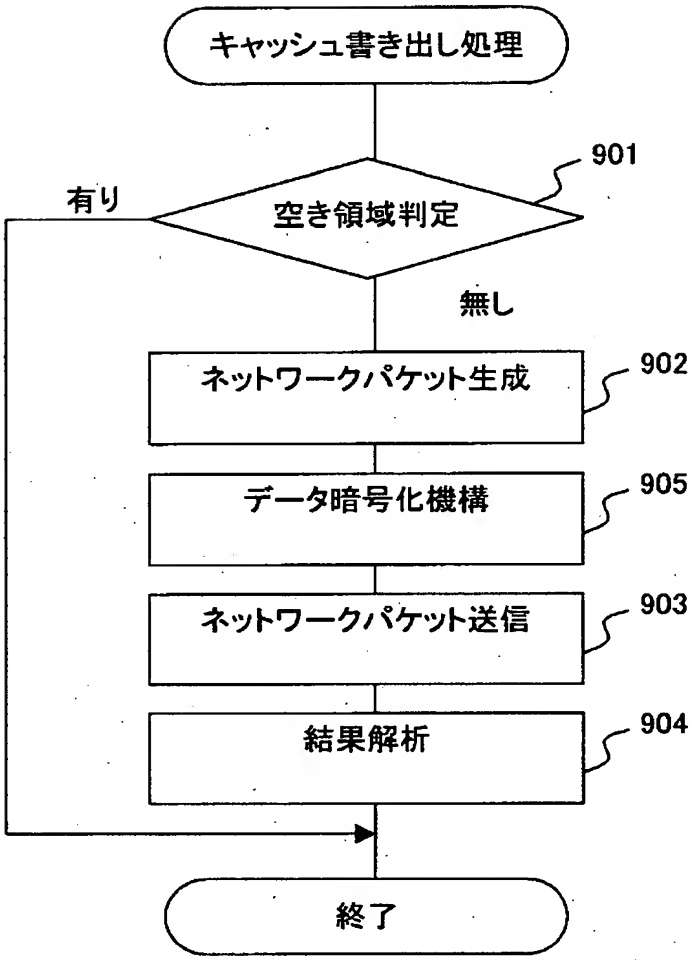
【図８】

図８



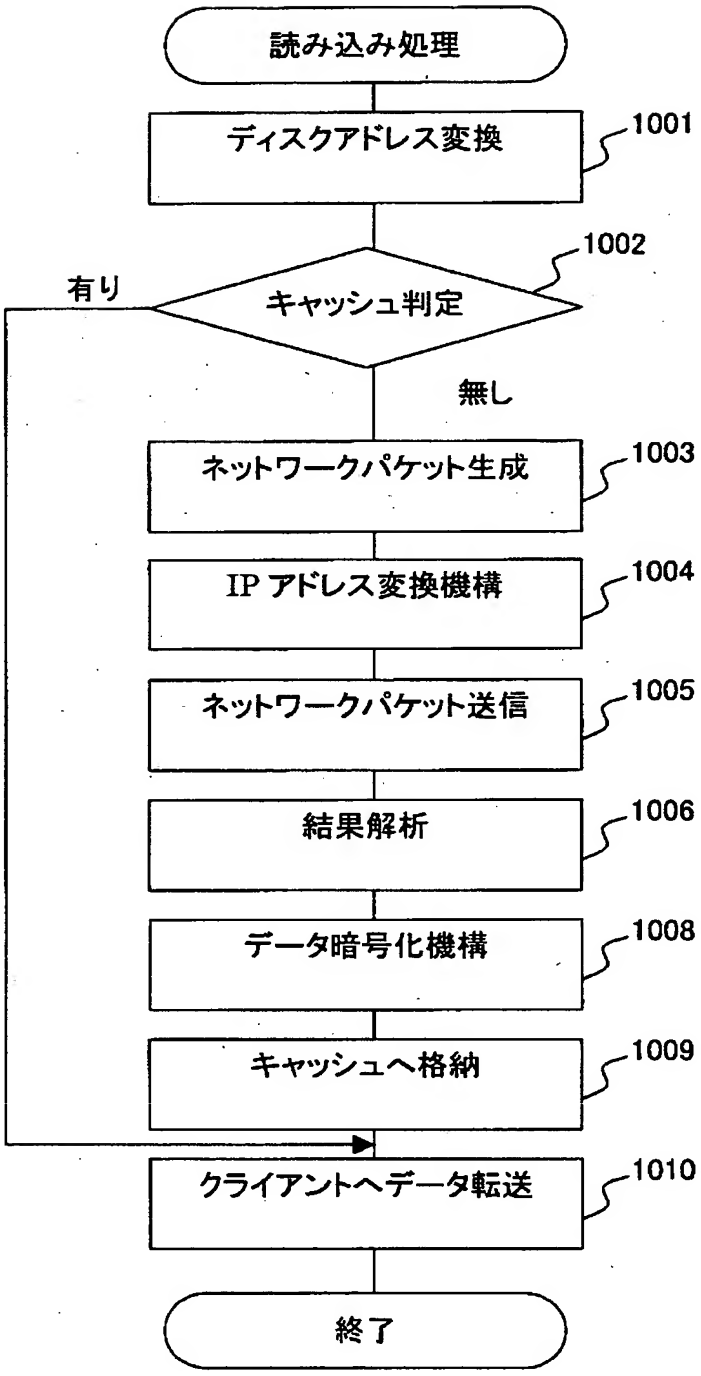
【図９】

図 9


キャッシュ書き出し処理
901
空き領域判定
有り
無し
ネットワークパケット生成
902
データ暗号化機構
905
ネットワークパケット送信
903
結果解析
904
終了

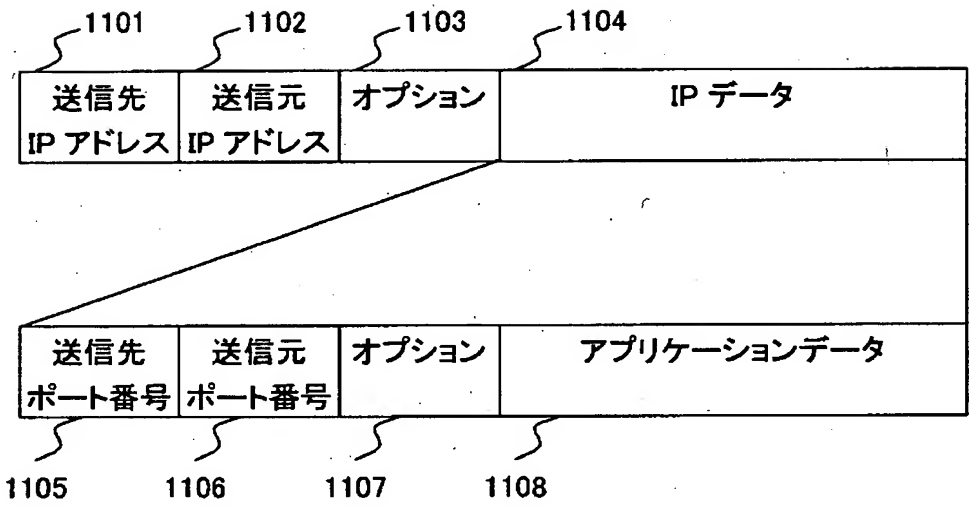
【図１０】

図 10


読み込み処理
ディスクアドレス変換
1001
キャッシュ判定
1002
有り
無し
ネットワークパケット生成
1003
IP アドレス変換機構
1004
ネットワークパケット送信
1005
結果解析
1006
データ暗号化機構
1008
キャッシュへ格納
1009
クライアントへデータ転送
1010
終了

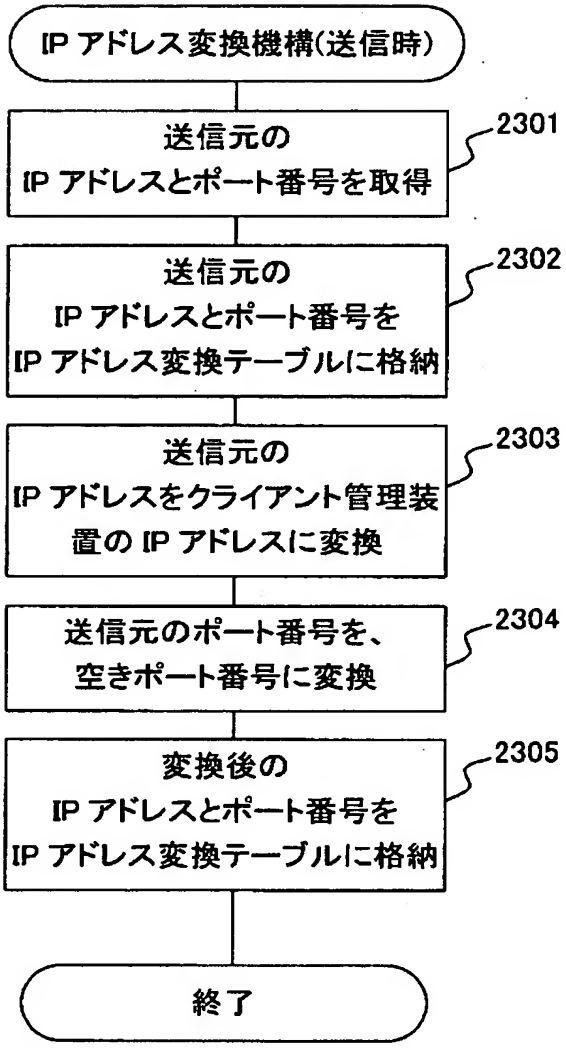
【図１１】

図 11


1101
1102
1103
1104
送信先 IP アドレス
送信元 IP アドレス
オプション
IP データ
送信先 ポート番号
送信元 ポート番号
オプション
アプリケーションデータ
1105
1106
1107
1108

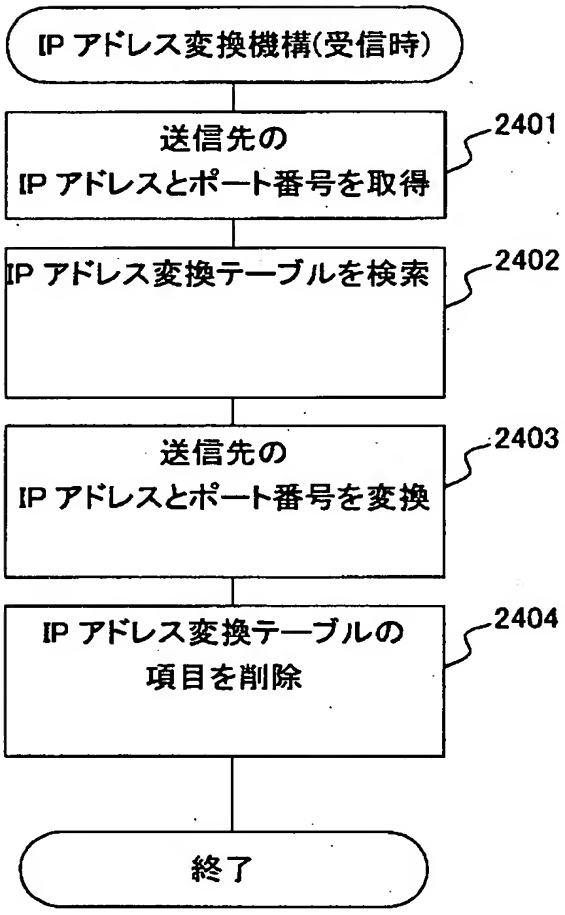
【図１２】

図 12


IP アドレス変換機構(送信時)
送信元の
IP アドレスとポート番号を取得
2301
送信元の
IP アドレスとポート番号を
IP アドレス変換テーブルに格納
2302
送信元の
IP アドレスをクライアント管理装置の IP アドレスに変換
2303
送信元のポート番号を、
空きポート番号に変換
2304
変換後の
IP アドレスとポート番号を
IP アドレス変換テーブルに格納
2305
終了

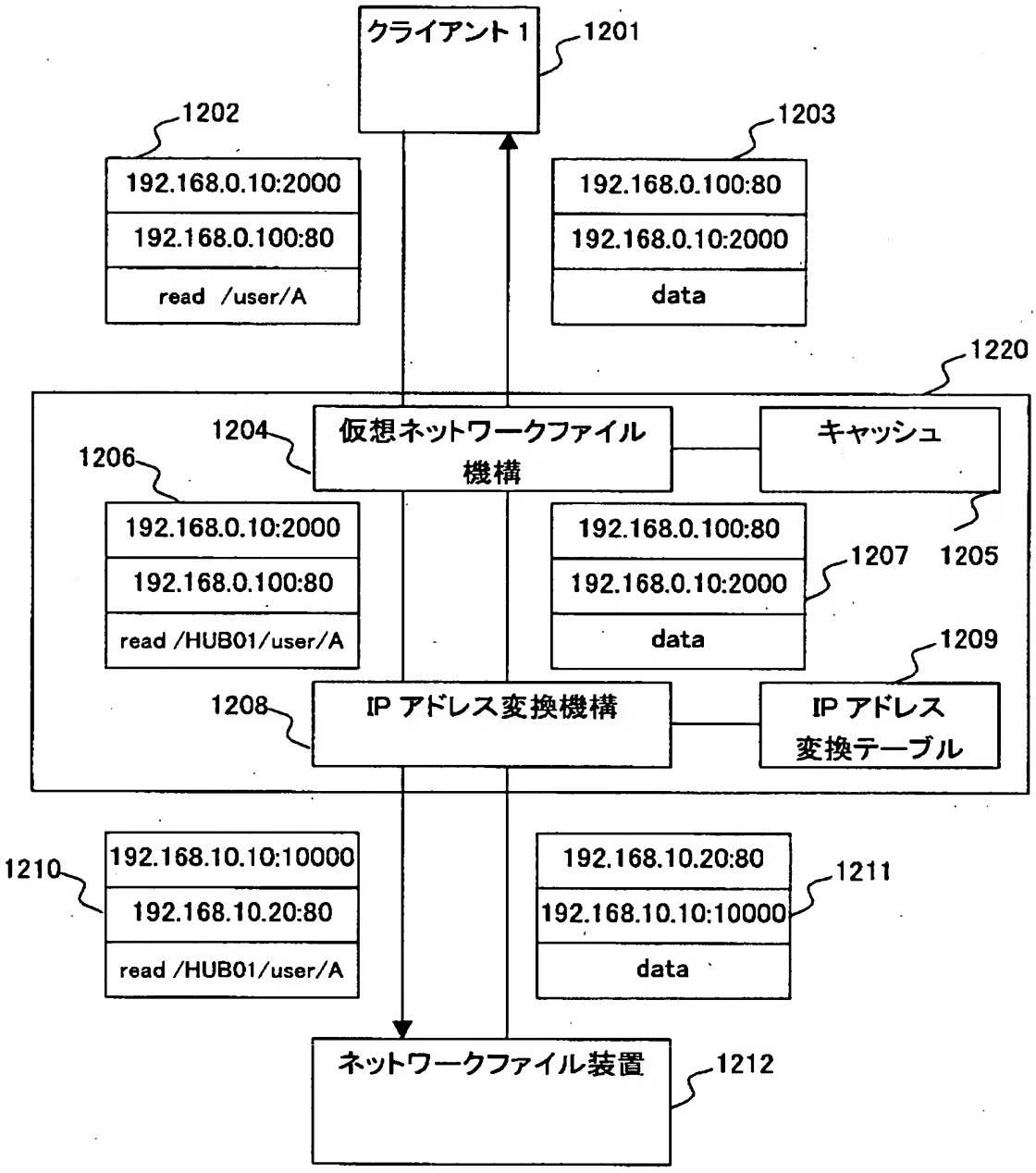
【図１３】

図 13


IP アドレス変換機構(受信時)
送信先の
IP アドレスとポート番号を取得
2401
IP アドレス変換テーブルを検索
2402
送信先の
IP アドレスとポート番号を変換
2403
IP アドレス変換テーブルの
項目を削除
2404
終了

【図１４】

図 14


クライアント 1
1201
1202
192.168.0.10:2000
192.168.0.100:80
read /user/A
1203
192.168.0.100:80
192.168.0.10:2000
data
1220
1204
仮想ネットワークファイル機構
キャッシュ
1206
192.168.0.10:2000
192.168.0.100:80
read /HUB01/user/A
192.168.0.100:80
192.168.0.10:2000
data
1207
1205
1209
1208
IP アドレス変換機構
IP アドレス変換テーブル
1210
192.168.10.10:10000
192.168.10.20:80
read /HUB01/user/A
192.168.10.20:80
192.168.10.10:10000
data
1211
ネットワークファイル装置
1212

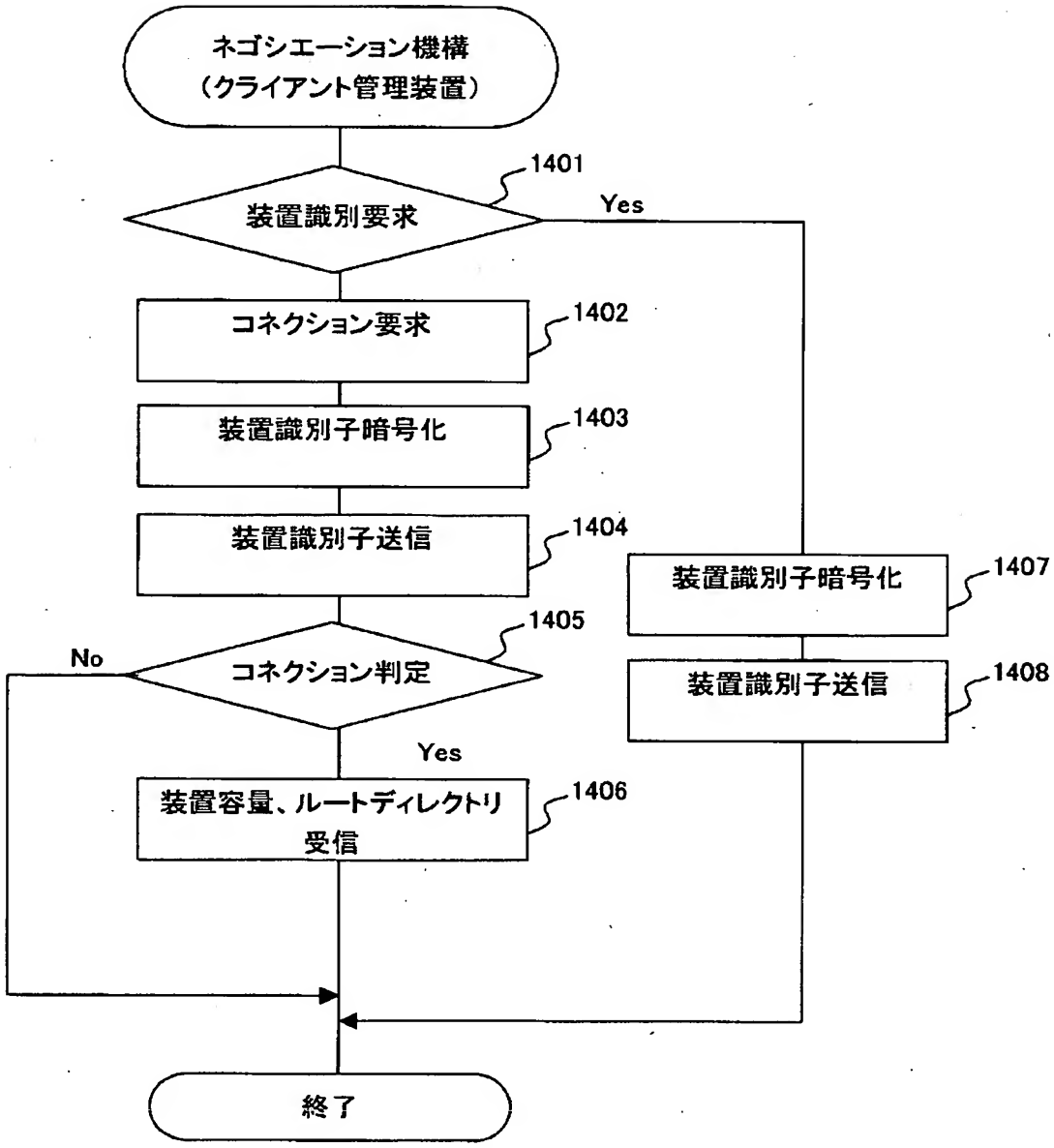
【図１５】

図 15

1301 クライアント IP アドレス	1302 クライアント ポート番号	1303 変換後 IP アドレス	1304 変換後 ポート番号
192.168.0.10	2000	192.168.10.10	10000
192.168.0.20	2001	192.168.10.10	10001
...	...	...	...

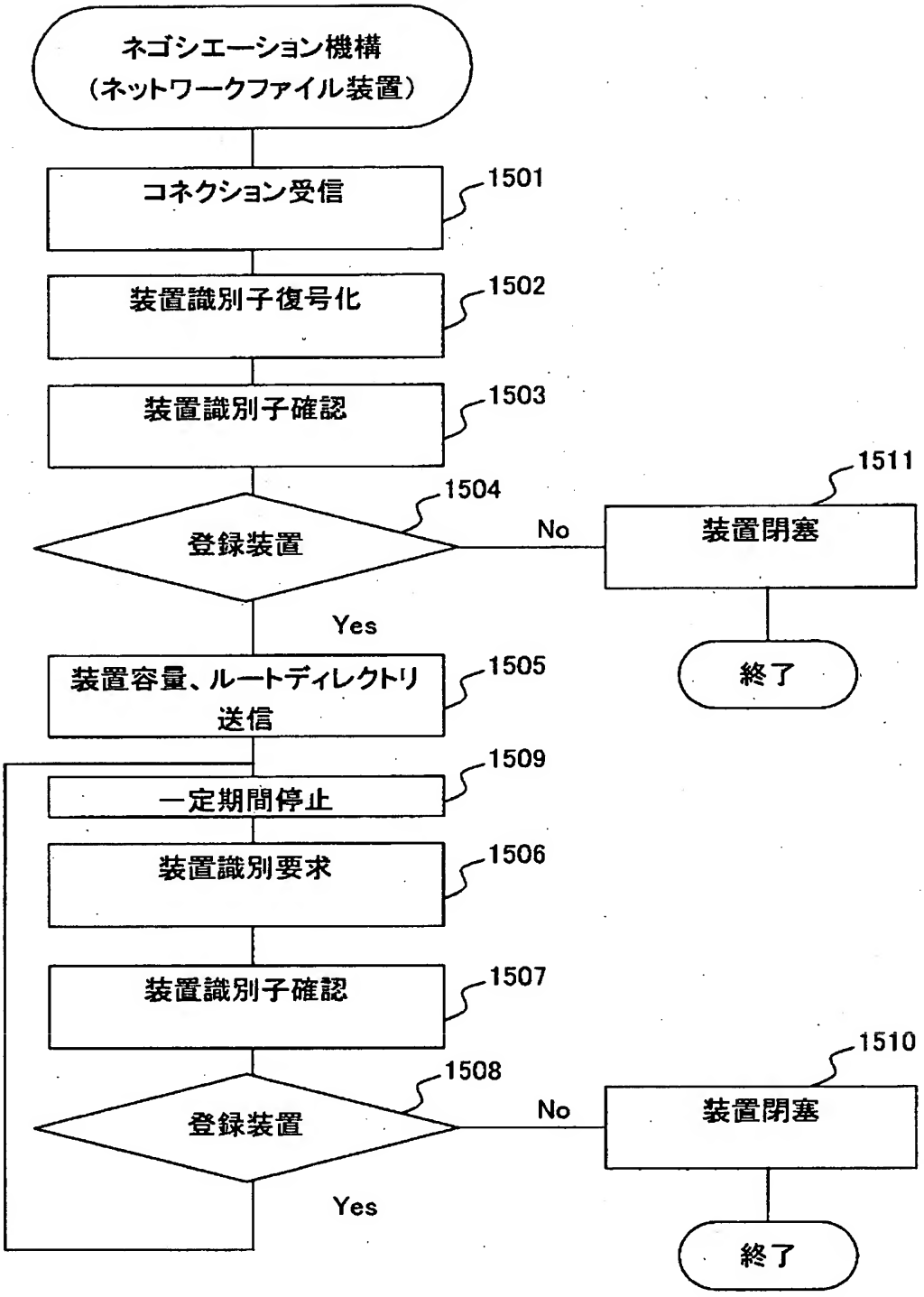
【図１６】

図 16


ネゴシエーション機構
（クライアント管理装置）
1401
装置識別要求
Yes
コネクション要求
1402
装置識別子暗号化
1403
装置識別子送信
1404
装置識別子暗号化
1407
1405
No
コネクション判定
装置識別子送信
1408
Yes
装置容量、ルートディレクトリ
受信
1406
終了

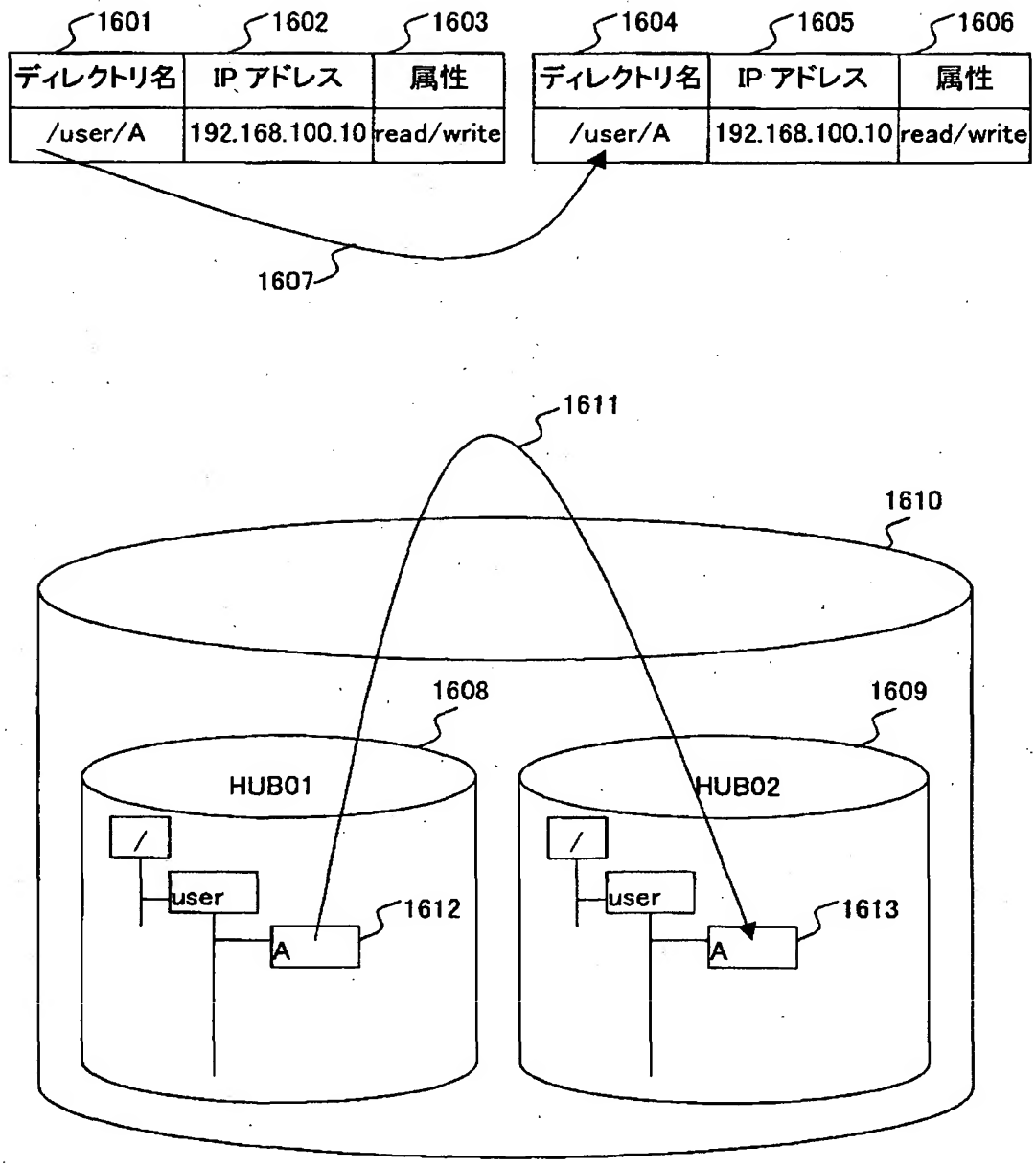
【図１７】

図 17


ネゴシエーション機構
（ネットワークファイル装置）
コネクション受信
1501
装置識別子復号化
1502
装置識別子確認
1503
登録装置
1504
No
装置閉塞
1511
終了
Yes
装置容量、ルートディレクトリ送信
1505
一定期間停止
1509
装置識別要求
1506
装置識別子確認
1507
登録装置
1508
No
装置閉塞
1510
終了
Yes

【図１８】

図 18


1601
1602
1603
1604
1605
1606
ディレクトリ名
IP アドレス
属性
/user/A
192.168.100.10
read/write
1607
1611
1610
1608
1609
HUB01
HUB02
/
user
A
1612
1613

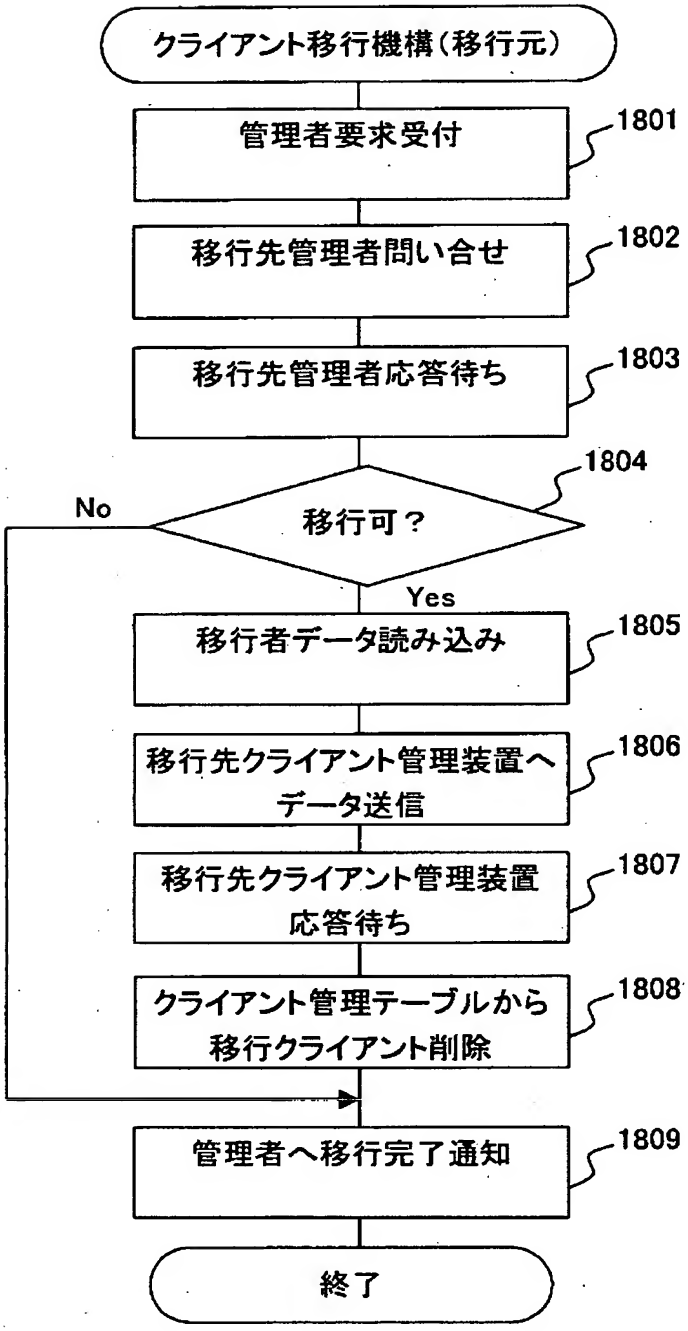
【図１９】

図 19

1701 ファイル名	1702 ユーザ識別子	1703 ファイル属性
/user/A/file1	501	rw
/user/A/file2	501	rwx
/user/B/file3	502	r
/user/C/file4	503	rw
/user/C/file5	503	rw

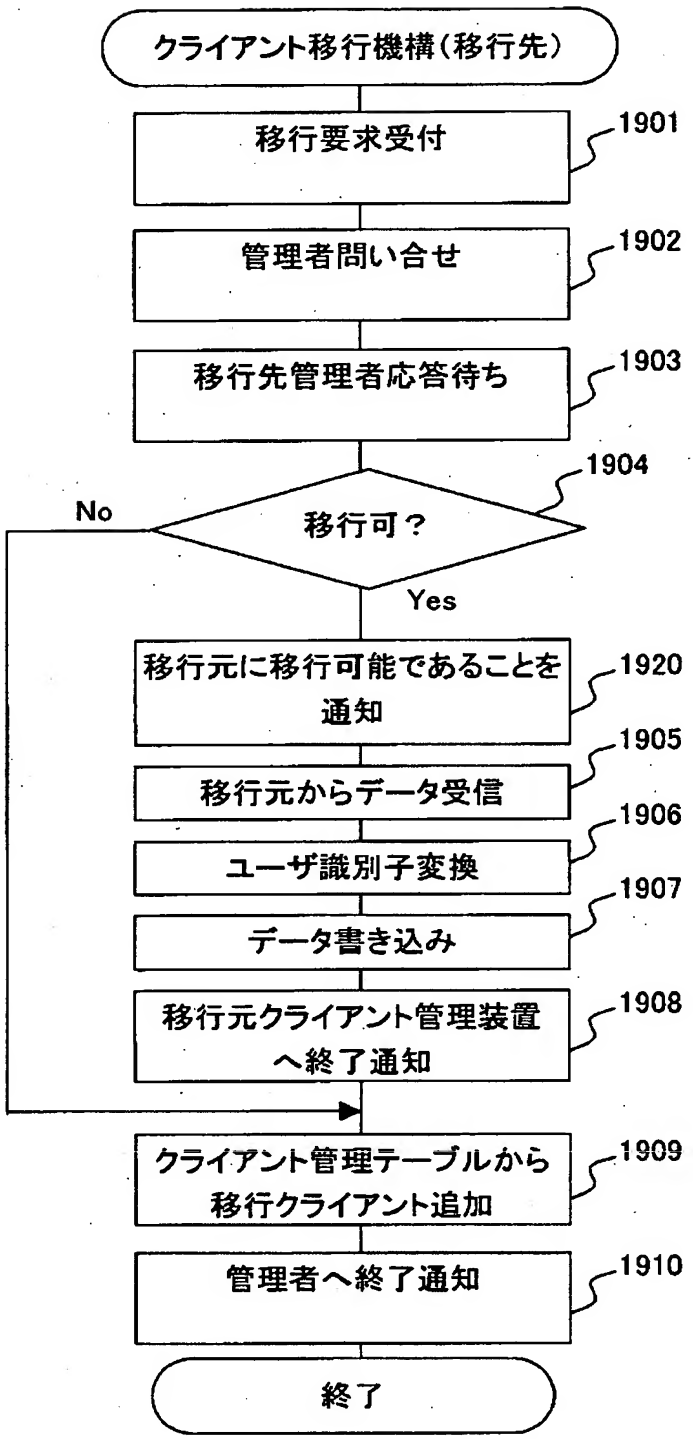
【図２０】

図 20


クライアント移行機構（移行元）
管理者要求受付
1801
移行先管理者問い合せ
1802
移行先管理者応答待ち
1803
移行可？
1804
No
Yes
移行者データ読み込み
1805
移行先クライアント管理装置へデータ送信
1806
移行先クライアント管理装置応答待ち
1807
クライアント管理テーブルから移行クライアント削除
1808
管理者へ移行完了通知
1809
終了

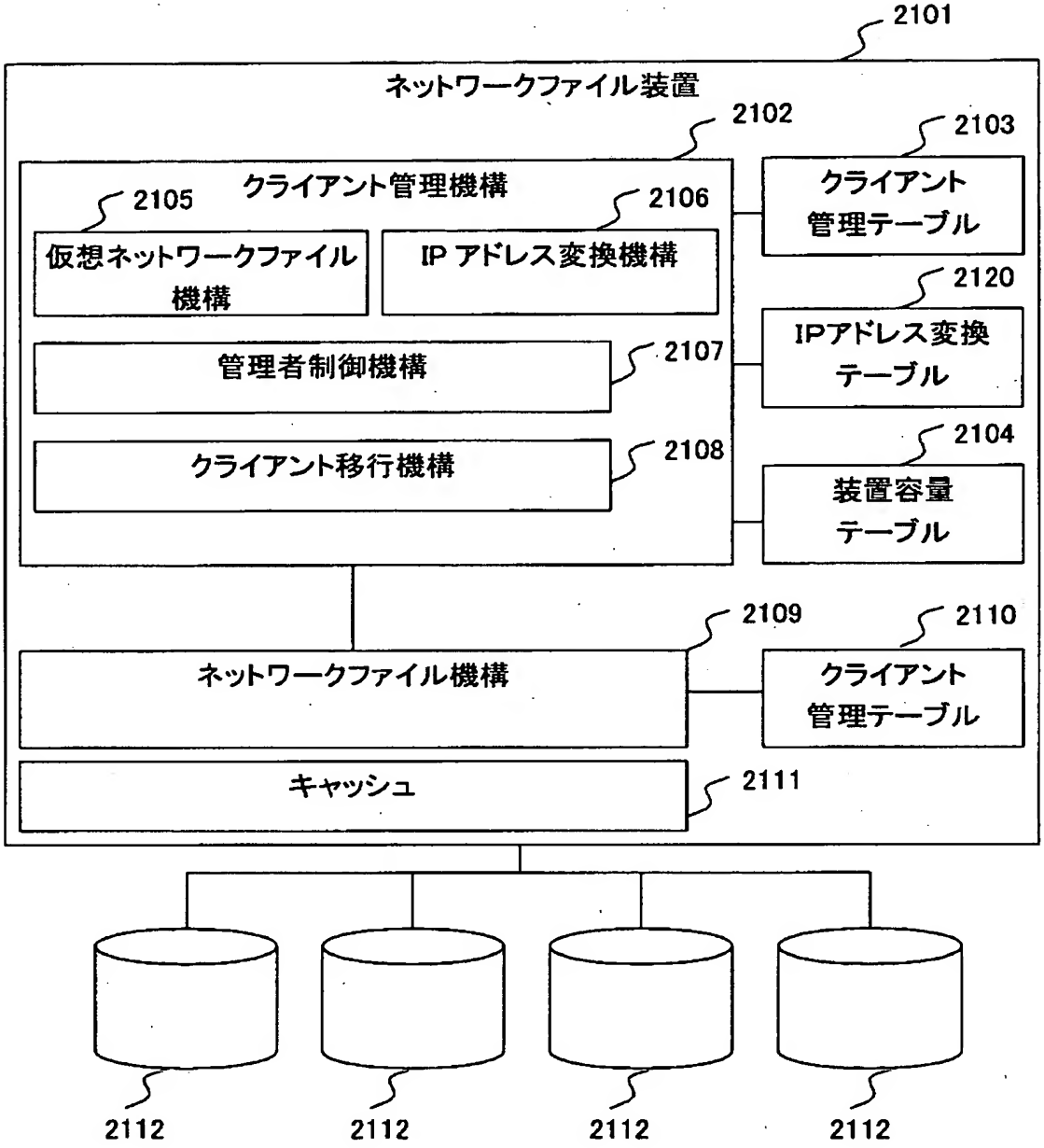
【図２１】

図 21


クライアント移行機構(移行先)
移行要求受付
1901
管理者問い合せ
1902
移行先管理者応答待ち
1903
移行可？
1904
No
Yes
移行元に移行可能であることを通知
1920
移行元からデータ受信
1905
ユーザ識別子変換
1906
データ書き込み
1907
移行元クライアント管理装置へ終了通知
1908
クライアント管理テーブルから移行クライアント追加
1909
管理者へ終了通知
1910
終了

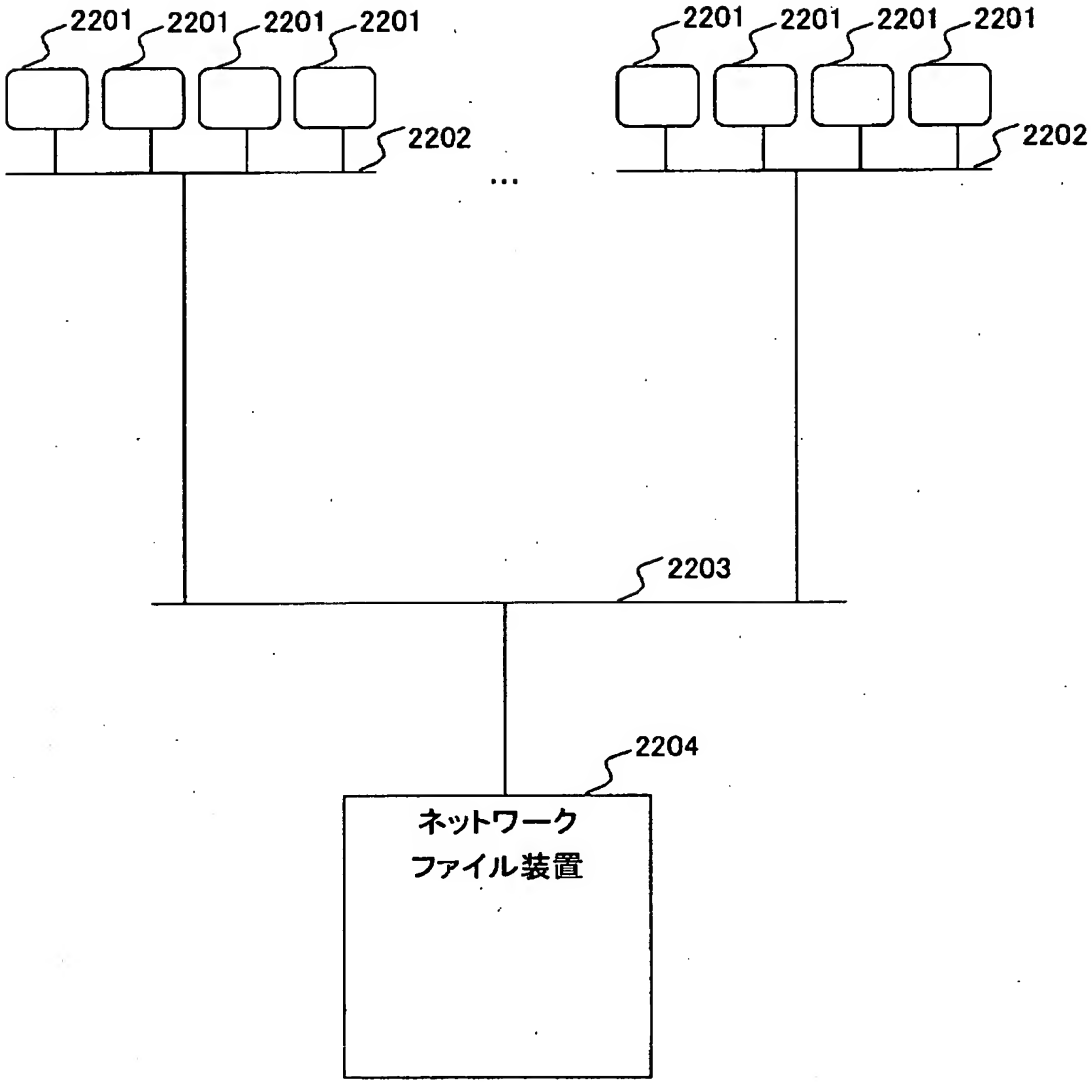
【図２２】

図 22


2101
ネットワークファイル装置
2102
クライアント管理機構
2105
仮想ネットワークファイル機構
2106
IP アドレス変換機構
2107
管理者制御機構
2108
クライアント移行機構
2103
クライアント管理テーブル
2120
IPアドレス変換テーブル
2104
装置容量テーブル
2109
ネットワークファイル機構
2110
クライアント管理テーブル
2111
キャッシュ
2112
2112
2112
2112

【図２３】

図 23


2201
2201
2201
2201
2202
...
2201
2201
2201
2201
2202
2203
2204
ネットワーク
ファイル装置

【書類名】　　要約書

【要約】

【課題】　大規模なネットワークファイル装置のクライアント管理を容易にする。

【解決手段】　ネットワークファイル装置とクライアントの間にクライアントを管理する装置を設け、管理を階層化する。

【効果】　大規模なクライアント環境でも、階層化することで各管理者は少ないクライアントの管理で済み、管理が容易になる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０１０５０９
受付番号	５０３０００７５２３７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　１月２１日

＜認定情報・付加情報＞

【提出日】　　平成15年 1月20日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所